REPUBLIC OF TURKEY
ISTANBUL GELISIM UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

Department of Electrical and Electronics Enginerring

DESIGNING AN ENHANCED USER AUTHENTICATED KEY MANAGEMENT SCHEME FOR 6G-BASED INDUSTRIAL APPLICATIONS

Master Thesis

IJAZ UL HAQ DARMAN

Supervisor
Asst. Prof. Dr. Musaria Karim MAHMOOD

Istanbul – 2022

THESIS INTRODUCTION FORM

Name and Surname	: Ijaz ul haq DARMAN
Language of the Thesis	: English
Name of the Thesis	: Designing An Enhanced User Authenticated Key Management Scheme for 6G-based Industrial Applications
Institute	: Istanbul Gelisim University Institute of Graduate Studies
Department	: Electrical and Electronics
Thesis Type	: Master
Date of the Thesis	: 03.08.2022
Page Number	: 75
Thesis Supervisors	: Asst. Prof. Dr. Musaria Karim MAHMOOD Assoc. Prof. Dr. Shehzad ASHRAF
Index Terms	: Sixth Generation (6G), Internet of Thing (IoT), Network in a Box (NIB), Security.

Turkish Abstract : Altıncı Nesil (6G) sistemde haberleşme sisteminde güvenliğin önemi daha da artmaktadır. 6G'nin potansiyel teknolojilerinden biri, Kutudaki Ağdır (NIB). 6G özellikli NIB, iletişim için kullanılan, çok nesilli, kolay ve hızlı bir şekilde kurulabilen bir teknolojidir. Donanım ve yazılıma dayalıdır. 6G özellikli NIB'nin temel özellikleri arasında düşük gecikme süresi ve yüksek düzeyde esneklik bulunur. Ayrıca sektördeki Battlefields veya afet durumları gibi afet durumlarında kullanılan uygulamalara bağlantı hizmeti vermektedir. Ancak, 6G özellikli NIB'de kullanılan uygulamaların çoğu uygun şekilde güvenli değildir. Güvenli olmayan kanal nedeniyle birkaç aktif ve pasif saldırı olasılığı vardır. Bu nedenle, bu tezde yeni bir uzaktan kullanıcı kimlik doğrulama ve anahtar yönetimi şeması sunulmaktadır. Bu şema, UAKMS-NIB'nin değiştirilmiş ve geliştirilmiş şemasıdır ve endüstriyel uygulamalarda kullanılan 6G etkin NIB kanalını güvence altına alan geliştirilmiş bir Bilinmeyen Kimlik Doğrulama Yönetim Planı (iUAKMS-NIB) olarak yeniden adlandırılmıştır. Bu nedenle önerilen şema, 6G haberleşme sistemindeki olası saldırılara karşı en iyi güvenlik çözümünü sunmaktadır. Sonuçlar, önerilen şemanın mevcut şemalarla karşılaştırıldığında daha iyi performans gösterdiğini göstermektedir.

Distribution List :

1. To the Institute of Graduate Studies of Istanbul Gelisim University
2. To the National Thesis Center of YÖK (Higher Education Council)

Ijaz ul Haq DARMAN

REPUBLIC OF TURKEY
ISTANBUL GELISIM UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

Department of Electrical and Electronics Engineering

DESIGNING AN ENHANCED USER AUTHENTICATED KEY MANAGEMENT SCHEMEFOR 6G-BASED INDUSTRIAL APPLICATIONS

Master Thesis

IJAZ UL HAQ DARMAN

Supervisor

Ass. Prof. Dr. Musaria Karim MAHMOOD

Istanbul – 2022

DECLARATION

I hereby declare that in the preparation of this thesis, scientific ethical rules have been followed, the works of other persons have been referenced in accordance with the scientific norms if used, there is no falsification in the used data, any part of the thesis has not been submitted to this university or any other university as another thesis.

Ijaz Ul haq DARMAN
…/…/2022

TO ISTANBUL GELISIM UNIVERSITY

THE DIRECTORATE OF GRADUATE EDUCATION INSTITUTE

The thesis study of Ijaz ul haq DARMAN Titled as Designing An Enhanced User Authenticated Key Management Schemefor 6G-based Industrial Applications has been accepted as MASTER THESIS in the department of Electrical and Electronics Engineering, By our jury.

Director	*Asst.Prof. Dr. Musaria Karim MAHMOOD* (Supervisor)
Member	*Assoc. Prof. Dr. Shafqat Ur REHMAN*
Member	*Asst.Prof. Dr. Ahmed Amin Ahmed SOLYMAN*

APPROVAL

I approve that the signatures above signatures belong to the aforementioned faculty members.

... / ... / 2022

Signature

Prof. Dr. İzzet GÜMÜŞ

Director of the Institute

SUMMARY

The 21st century is the era of modern technologies and communication, with the organization of Security Group (SG) frameworks. On the other hand, the development of Sixth Generation (6G) frameworks is under process. In 6G networks, the trend toward cloud and edge native infrastructures is projected to continue, necessitating comprehensive 6G network security architecture design. Network in a Box (NIB) is a dynamic solution for mobile communication that is becoming more popular nowadays. Because it can be transported in a bag, it is sometimes also referred to as "Network in a Bag". A multi-generational technology includes technologies from the first to the sixth generations. These technologies include technologies from the first through the second, third, fourth, fifth, and sixth generations. The NIB is a collection of both the hardware and software components for mobile communication that are simple to set up and maintain. The fundamental concept behind the use of NIB is to give communication services in catastrophe scenarios such as earthquakes, fires in industries, battlefields, floods, and other types of emergency situations, among others. The concept if NIB relies on merging all sorts of Modules for both System requirements needed for cellular operators were packed into a limited wide range of physical devices in a single backpack. This highly flexible 6G-enabled NIB can offer connection services for a wide range of applications (for example, "after catastrophic scenario," "battlefield scenario," and "industrial scenario") due to its high degree of adaptability. It is important to note that emergency as well as Military networks are designed to be both adaptable and versatile., owing to the fact that the Although the implementation of these networks is not completely understood. They are classified as "Mobile Ad-hoc Networks (MANETs)" in this category. Furthermore, NIB is a portable entity by nature. As a result, it may be used in disaster management situations such as earthquakes and tsunamis.

Recently, standards for emergency and tactical networks have been created that can enable systems with a smaller number of physical devices while still achieving the prime objective of improving viability. Many network providers have also adopted this approach in order to build these networks, which may be set up with just a small number of physical devices, or even just a single device. Because of this, NIB develops an alternative network communication technology that will be able to meet the needs of innovative mobile systems whcih is Communication network for industrial use and Earthquake . As a general rule, the 6G-enabled NIB may be "configured to function either totally independently or in conjunction with other older network components or other NIBs." It also designed to accomplish availability for all wireless networks in a tiny, compact, and portable package for business, commercial, private, government, and military applications.

6G-enabled "Evolved packet core (EPC)," "tower with antenna," "user with a mobile device," "IP Multimedia Subsystem (IMS)," "content server, "smart industrial devices," and "trusted authority" are just a few of the components that make up an NIB that is used in industrial applications. All of these components make it easier for a user to communicate with additional users or to get essential forms of service, such as web-based information, media capabilities, as well as data collected from intelligent manufacturing equipment, among other things. For the purpose of monitoring and regulating industrial equipment, smart industrial tools are being used. 6G wireless communication technology makes it possible for various components and devices to communicate with one another. The main features of 6G-enabled NIB include low latency and a high level of flexibility. In addition, it provides connectivity services to the applications used in the disaster situations such as Battlefields or disaster situations in the industry. However, most of the applications used in 6G-enabled NIB are not appropriately secured. There are chances of several active and passive attacks due to the insecure channel. Therefore, a novel remote user authentication and key management scheme is presented in this thesis. This scheme is the modified and improved scheme of UAKMS-NIB and renamed as an improved Unknown Authentication Management Scheme (iUAKMS-NIB) that secures the 6G-enabled NIB channel used in industrial applications. Hence, the proposed scheme provides the best security solution against the possible attacks in the 6G communication system. The results show that the proposed scheme performs better when compared with the existing schemes.

Key Words: Sixth Generation (6G), Internet of Thing (IoT), Network in a Box (NIB), Security.

ÖZET

21. yüzyıl, Güvenlik Grubu (SG) çerçevelerinin organizasyonu ile modern teknolojiler ve iletişim çağıdır. Öte yandan, Altıncı Nesil (6G) çerçevelerinin geliştirilmesi devam etmektedir. 6G ağlarında, kapsamlı 6G ağ güvenliği mimarisi tasarımı gerektiren bulut ve uç yerel altyapılara yönelik eğilimin devam etmesi bekleniyor. Network in a Box (NIB), günümüzde daha popüler hale gelen mobil iletişim için dinamik bir çözümdür. Bir çantada taşınabildiği için bazen "Çantadaki Ağ" olarak da anılır. Çok nesilli bir teknoloji, ilk nesilden altıncı nesile kadar olan teknolojileri içerir. Bu teknolojiler, birinci nesilden ikinci, üçüncü, dördüncü, beşinci ve altıncı nesillere kadar olan teknolojileri içerir. NIB, mobil iletişim için kurulumu ve bakımı basit olan hem donanım hem de yazılım bileşenlerinin bir koleksiyonudur. NIB kullanımının arkasındaki temel kavram, diğerleri arasında depremler, endüstrilerdeki yangınlar, savaş alanları, sel ve diğer acil durum türleri gibi felaket senaryolarında iletişim hizmetleri vermektir. NIB'nin konsepti, mobil ağların gerektirdiği her türlü yazılım ve donanım modülünü az sayıda fiziksel cihaz içeren tek bir çantada birleştirmeye dayanıyor. Bu son derece esnek 6G özellikli NIB, yüksek düzeyde uyarlanabilirliği sayesinde çok çeşitli uygulamalar için (örneğin, "felaket senaryosu sonrası", "savaş alanı senaryosu" ve "endüstriyel senaryo") bağlantı hizmetleri sunabilir. Acil durum ve taktik ağların, bu ağların konuşlandırılmasının iyi anlaşılmadığı gerçeğinden dolayı, uyarlanabilir olduğu kadar esnek olacak şekilde inşa edildiğini belirtmek önemlidir. Bu kategoride "Mobil Ad-hoc Ağlar (MANET'ler)" olarak sınıflandırılırlar. Ayrıca, NIB doğası gereği taşınabilir bir varlıktır. Sonuç olarak deprem ve tsunami gibi afet yönetimi durumlarında kullanılabilir.

Son zamanlarda, daha az sayıda fiziksel cihaza sahip sistemlere olanak sağlarken aynı zamanda canlılığı iyileştirme ana hedefini gerçekleştirebilen acil durum ve taktik ağlar için standartlar oluşturulmuştur. Pek çok ağ sağlayıcısı, sadece az sayıda fiziksel cihazla veya hatta sadece tek bir cihazla kurulabilen bu ağları kurmak için bu yaklaşımı benimsemiştir. Bu nedenle NIB, yeni nesil mobil ağların (yani endüstriyel kullanım ve Deprem için iletişim ağı) ihtiyaçlarını karşılayabilecek alternatif bir ağ iletişim teknolojisi geliştirmektedir. Genel bir kural olarak, 6G özellikli NIB, "tamamen bağımsız olarak veya diğer eski ağ bileşenleri veya diğer NIB'ler ile birlikte çalışacak şekilde yapılandırılabilir". Ayrıca iş, ticari, özel, devlet ve askeri uygulamalar için küçük, kompakt ve taşınabilir bir pakette tüm kablosuz ağlar için kullanılabilirliği sağlamak üzere tasarlanmıştır.

6G özellikli "Gelişmiş paket çekirdek (EPC)," "antenli kule", "mobil cihazlı kullanıcı", "IP Multimedya Alt Sistemi (IMS)," "içerik sunucusu, "akıllı endüstriyel cihazlar" ve "güvenilir otorite" endüstriyel uygulamalarda kullanılan bir NIB'yi oluşturan bileşenlerden sadece birkaçıdır.Bu bileşenlerin tümü, bir kullanıcının diğer kullanıcılarla iletişim kurmasını veya web tabanlı bilgi, multimedya hizmetleri gibi önemli hizmetleri almasını kolaylaştırır. veya akıllı endüstriyel ekipmanlardan gelen veriler, diğer şeylerin yanı sıra.Endüstriyel ekipmanların izlenmesi ve düzenlenmesi amacıyla akıllı endüstriyel araçlar kullanılmaktadır.6G kablosuz iletişim teknolojisi, çeşitli bileşenlerin ve cihazların birbirleriyle iletişim kurmasını mümkün kılar.Temel özellikleri 6G özellikli NIB, düşük gecikme süresi ve yüksek düzeyde esneklik içerir.Ayrıca, endüstrideki Battlefields veya afet durumları gibi afet durumlarında kullanılan uygulamalara bağlantı hizmetleri sağlar.Ancak çoğu 6G özellikli NIB'de kullanılan uygulamaların çoğu uygun şekilde güvenli değildir. Güvenli olmayan kanal nedeniyle birkaç aktif ve pasif saldırı olasılığı vardır. Bu nedenle, bu tezde yeni bir uzaktan kullanıcı kimlik doğrulama ve anahtar yönetimi şeması sunulmaktadır. Bu şema, UAKMS-NIB'nin değiştirilmiş ve geliştirilmiş şemasıdır ve endüstriyel uygulamalarda kullanılan 6G etkin NIB kanalını güvence altına alan geliştirilmiş bir Bilinmeyen Kimlik Doğrulama Yönetim Planı (iUAKMS-NIB) olarak yeniden adlandırılmıştır. Bu nedenle önerilen şema, 6G haberleşme sistemindeki olası saldırılara karşı en iyi güvenlik çözümünü sunmaktadır. Sonuçlar, önerilen şemanın mevcut şemalarla karşılaştırıldığında daha iyi performans gösterdiğini göstermektedir.

Anahtar kelimeler: Altıncı Nesil (6G), Nesnelerin İnterneti (IoT), Kutuda Ağ (NIB), Güvenlik

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

CHAPTER TWO
BACKGROUND STUDIES

CHAPTER THREE
SYSTEM MODEL

CHAPTER FOUR
THE WAZID ET AT.'S UAKMS-NIB SCHEME

CHAPTER FIVE
PROPOSED SCHEME

CHAPTER SIX
PERFORMANCE ANALYSİS

ABBREDIVATIONS

TERM	**:**	**ACRONYMS**
1G	**:**	First Generation
2G	**:**	Second Generation
3G	**:**	Third Generation
4G	**:**	Fourth Generation
5G	**:**	Fifth Generation
6G	**:**	Sixth Generation
AES	**:**	Advanced Encryption Standard
AI	**:**	Artificial Intelligence
DMM	**:**	Distributed Mobility Management
DSL	**:**	Digital Subscriber Link
ECC	**:**	Eliptic Curve
eMBB	**:**	Enhanced Mobile Broadband
eNB	**:**	evolved Node Base Station
gNB	**:**	Next Generation Node Base Station
GRA	**:**	Grey Relational Analysis
HetNet	**:**	Heterogeneous Network
IMS	**:**	IP Multimedia Subsystem
IoT	**:**	Internet of Things

IP	**:**	Internet Protocol
iUAKMS	**:**	Inhanced Unknown Authentication Management
KNN	**:**	K Nearest Neighbours
LIS	**:**	Large Smart Surface
LSTM	**:**	Long Short-Term Memory
LSTM	**:**	Long Short-Term Memory
LTE	**:**	Long Term Evolution
MANETS	**:**	Mobile Ad-Hoc Networks
MD	**:**	Mobile Device
MIMO	**:**	Multiple Input Multiple Output
MME	**:**	Mobility Management Entity
NAS	**:**	Non-Access Stratum
QoE	**:**	Quality of Energy
QoS	**:**	Quality of Service
RAN	**:**	Radio Access Network
RAT	**:**	Radio Access Technology
SDN	**:**	Software-Defined Networking
TA	**:**	Trustworthy Authorities
THz	**:**	Terahertz
UKMAS	**:**	Unknown Authentication Management System

URLLC	**:**	Ultra-Reliable Low Latency Communication
VLC	**:**	Visible Light
VoIP	**:**	Voice Over IP
WLAN	**:**	Wireless Local Area Network
XR	**:**	Extendent Reality
3GPP	**:**	Third Generation Partnership Project
HSS	**:**	Home Subscriber Server

LIST OF TABLES

LIST OF FIGURES

PREFACE

I express my sincere gratitude to my beloved parents, especially my brother Engr. Riaz Darmal, who provide me support for surviving in this world with confidence after almighty Allah. I wouldn't be successful without their love, care and guidance.

I am so thankful to my honourable and respected supervisor Dr. Musaria Karim Mahmood, for his continuous support guidance and contribution to my work. He was so kind and cooperative during my research work.

I am also grateful to Dr. Shehzad Ashraf for his guidance, help and support. It would not be possible to complete my thesis without his kind help and assistance.

Last but not least, I am very grateful to my entire teaching faculty of the Electrical and Electronics Engineering Department at Istanbul Gelisim University (IGU), Turkey.

CHAPTER ONE

INTRODUCTION

In the framework of the Fifth Generation (5G), researchers focus on the versatile organization of the Sixth Generation (6G). Keeping up with the deployment of a new generation of cellular systems every decade or so, the likelihood of 6G system deployment is expected to be implemented in the year or before 2030 (Viswanathan & Mogensen, 2020). Due to the difficulty of commercializing new technologies, it is time to begin studying the 6G technology components. Since 2018, scientists have been concentrating their efforts on the 6G idea and its applications (Gui et al., 2020). Anticipating the shortcomings of 5G, in March 2019, the world's first 6G summit was held in Finland. Prepared the first white paper on 6G, the basis for research in 6G network lied. Since then different governments and organizations have announced the entry of research projects into 6G network. For example, the UK government invests in the research of this new technology The Finnish Academy announced its interest in conducting basic research. 6G focuses; higher data rate, low latency and static reliability, improve connectivity, increase system capability, expand spectrum efficiency, increase energy efficiency, support security, and recognize intelligence (M. Wang et al., 2020). So far, there is no specific standardization of the 6G network, just many possibilities and possibilities. Many argue that 6G should be much more than just an advancement of SG (Chen et al., 2020). For example, in 6G, coverage should increase, providing full-area underwater coverage with more Artificial Intelligence (AI) capabilities. From the point of view of many experts, AI should be the main component of the 6G network, a combination of the architecture and emerging AI tools and network roles. 6G is intended to be three-dimensional networks including space-air-land-ocean with different types of partitions, powered by new technologies and standards to make the system more intelligent and flexible (C.-X. Wang et al., 2020). As 6G networks are increasingly coUmplex, heterogeneous and dynamic, effective resource utilization, consistent client experience, automatic management and orchestration are extremely difficult to achieve (Zhang & Zhu, 2020). 6G is likely to support a variety of new Internet of Everything (loE) applications, such as eXtended Reality (XR), holographic communication, smart conditions, brain-computer interactions, connected robots, autonomous systems, wireless brain-computer interactions, block chain and Distributed ledger. Emerging technologies such as ultra-large Multiple-input multiple-output (MIMO) (Ylianttila et al., 2020), holographic beam forming, large smart surfaces (LIS). New network paradigms, Terahertz (THz) communication, visible light communication (VLC) and smart radio, AI local architecture and space-land-ocean integrated 3D networks are being studied extensively. The 6G network must be flexible enough to provide specialized services in dynamic situations. However, it is very difficult to realize the complex system efficiently with traditional manual approaches. There were many extraordinary challenges to design and develop space-air-ground integrated networks with different types of radio access technologies (Gui et al., 2020). From the research, four types of 6G core services were identified for enhanced performance along with 5G. These include the advanced mobile sibling. ad band (eMBB), + ultra-reliable low latency communication (URLLC), advanced eMBB + large machine type communication (MMTC), advanced URLLC + MMTC, and advanced EMBB + URLLC + MMTC based on tradeoff (Viswanathan & Mogensen, 2020). 6G will operate in the terahertz (THz) bands from 100GHZ to 10THZ to provide a peak data rate of 1000 gigabits per second with air latency of under 100 microseconds. 6G will have the potential to be faster than current 5G, be 100 times more reliable, and offer broad coverage while supporting ten times more devices per square kilometer. 5G communications are currently in use, with more compatibility and More features than fourth-generation communication. However, by 2030, support for AI is approaching in the world of communications and networking. Although 6G still has some problems, it is expected to be released soon. AI in this perspective, terahertz communication, Usable capacity, visual wireless technology, and other terms Wireless data integration and energy transmission, integration, optical network, block chain, three-dimensional networking, quantum communication, unmanned aerial vehicle, cell-free communications, big data analytics helping to support 6G architecture guarantee in sensing and communication, integration of access back haul networks, dynamic networks licensing, holographic beam forming and QoS. These features are relevant to its industrial application. There is a wide variety of expected applications as a result (Wikström et al., 2020). Due to the drawbacks of the 5G mobile system as a platform for Internet of Everything (IoE) applications, global research efforts are currently focused on the 6G wireless system.

The IoE's potential is huge, and it's only becoming bigger. With the arrival of the fifth industrial revolution, the IoE is evolving into Industrial IoE (IIoE) projects.

By and large this technology will have vast opportunities to apply it to a wide spectrum of industry with its AI and other features. Defense industry will become more cutting edge and can spark a competition like the one ignited by the stealth technology between the US and China. However, it is apparently being researched in good faith to accelerate the growth, quality and performance of a wide range of industries. In industrial application this can worth for securing the communication to encounter the Third person or fake information can be detecting in the channel. According to research, some of the most important considerations for 6G include High data rates in dense installations, network hardness under tough circumstances, and a reduction in delay at maximum throughput are just a few of the benefits of this technology. Overall cost has been greatly decreased (TCO) every bit and serviced area, getting where connection is required, and end-to-end protection that complies with market demands are all important considerations. It is foreseen that six new possible technological transformations to shape the 6G system: The AIML-based communication design and optimization (ii) expansion into new spectrum bands and new smart spectrum sharing methods (iii) system definition with localization and sensing capabilities (iv) meeting high latency and reliability performance requirements (v) (Sun et al., 2020). Sustainability, believably, ubiquitous service coverage, extreme applications and performance, related smart systems, and network computing fabric are expected to be the major difficulties for a 6G time frame.

1.1. Six Generation Impact on Human Lives

6G will have a great impact on human lives as compared to other generations because of its low latency and use of high frequency, which is about the integration of sensing communication and programming. With the help of digital tools, it can be executed to control the crimes happening in the digital world. When a user enters the physical world, the main needs will be security and safety. The safety of the people will be dependent on security. 6G terminals networks support high bit rates and other hand the attackers have a powerful tool and many critical infra use case is industry, health, traffic IoT manufacturers have a business interest to gain access to usage data. And the human experience across the world is ten, it means value, sense, intent, knowledge, privacy and trust, choice, time, inclusion, affordability, sustainability. The future communications with 6G will be high resolution mapping and mixed reality co-design it will have air interface, new spectrum technology, network as a sensor, extreme connectivity, security and trust.

However, in AI Centrex 6G network architecture where is the convergence of communication and computing the biggest challenge is computation model in the respect studies shows in the deep learning computing era the polynomials to train our model is less than 5% of error rate is expected to have a ten billion dollars of computing cost. Expected usage of 6G in 2030 will be; wearable devices, gesturing and talking to gadgets rather than touchpad, devices will be smart enough and will be aware of its context, and the network will become ever more sophisticated at calculating our requirements, self-sufficient automobiles, wireless cameras as sensors AI, innovative practices will be used in security-screening events to eradicate security lines, crypto cash and keys, various home facility robots, health care will be significantly transformed, with 24/7 checking of vital factors for both normal healthy and patient through numerous wearable devices, robotic swarms drones usage will be common among various infrastructures such as hospitals, warehouse, restaurants and package delivery. Dynamic digital twins in the digital world with increasingly accurate, synchronous updates of the physical world will be an essential platform for augmenting human intelligence (Sarieddeen et al., 2019). Foreseeable challenges for 6G implementation are; Peak Data rate, Latency and Reliability, Spectrum Efficiency, Energy efficiency, Promote Security. Network Intelligence (4).

1.2. Security in 6G

In critical regions of the 6G network, certain essential technologies are already proving effective. They provide high dependability, low latency, and secure and efficient transmission services to 6G networks. Al, Molecular Communication, Quantum Communication, Block Chain, and Terahertz Technology are among of these technologies (THz). Communication through Visible Light (VLC) (Basar, 2019). Wireless network security concerns at the cyber and physical layers are common in everyday life. As a result, wireless computing is becoming more popular among people and communities. Constant data uploading, caching, and sending is a major source of privacy leaks. A critical goal is to provide wireless computing with secure communications. As a result, security should be regarded a fundamental performance requirement of wireless computing in 6G. 6G system is intended to support numerous new applications with emerging technologies paradigms and models. However, many technical concerns need to be addressed to accomplish the objective of 6G system. With new attacks, 6G networks will face various new challenges and security threats. Open nature of wireless channel is particularly vulnerable to malicious attacks. Giving remote processing with trusted communications is a critical goal. Therefore, security ought to be considered as basic performance constraint of wireless computing in 6G (Akyildiz et al., 2014). In recent years issues on networks security and According to (AVISPA, 2015), authentication, access control, hostile behavior, encryption, and communication are the key concerns with 6G security and privacy. Furthermore, risk mitigation should be an essential component of the design, since network security and privacy have grown increasingly crucial in recent years. Authentication, access control, malicious assaults, sustainability, credibility, ubiquitous service coverage, extreme applications and performance, linked intelligent systems, and network computing fabric are all susceptible components of the 6G system (Chowdhury et al., 2020), but few technologies are sensitive to certain subjects, like VLC is weak against malicious attacks and data transmission. The molecular communication and the THz technology are concerned with security and privacy matters. Authentication, encryption, and communication problems plague the former, while authentication security and malicious assaults plague the latter. Distributed AI and intelligent radio intersect with block chain technology and quantum communication.

6G has inherited and novel threats, Machine learning (ML) can be used to make safer systems, but also more dangerous attacks, ML is a tool and risk in 6G (Padhi & Charrua-Santos, 2021) Authentication, encryption, and communication problems plague the former, while authentication security and malicious assaults plague the latter. Distributed AI and intelligent radio intersect with block chain technology and quantum communication. The network's wire line-grade reliability also implies that additional security and privacy safeguards must be implemented (Strinati et al., 2019). In industrial networks Jamming is a new threat that need to be addressed, physical security will not be adequate if attackers and hackers attempt to jam networks from outside industrial capacity or it can simply cause delay in communications and cause serious problems on time-sensitive networks. Therefore, second level authentication might be required, which in turns will be crucial to handle different networks communications (Canetti & Krawczyk, 2001).

1.3. Motivation

There are several benefits to using a 6G-enabled NIB in comparison to previous wireless communication technologies, but there are also network security concerns with regard to the forthcoming 6G-enabled wireless networks (i.e., NIB). This occurs as a result of the fact that security measures are not completely implemented in modern wireless communication networks, such as 6G. According to the findings of various research investigations, Third person attacks are now possible because to a newly discovered capability. in "terahertz-based 6G networks," which may be exploited. The fact that "6G enabled NIB implemented for industrial applications" may provide a wide range of user privacy options. vulnerabilities is very essential to emphasize since it may be subject to a variety of different forms of cyberattacks. It is possible to conduct a variety of attacks on a 6G-enabled NIB that is being used for industrial applications. These attacks include Attacks such as replay, third person, third person , disclosure of confidential information, and unlawful session key calculation, unauthorized insider, and stolen smart industrial device are examples of such vulnerabilities.

. As a result, security procedures must be built in a "6G-enabled NIB that are used for industrial applications," as described above. To access real-time data, a registered user must also authenticate with the smart industrial devices that are being used to gather the information. Disaster management (earthquakes and tsunamis), for example, is one of the important applications of NIB, where a user has to be able to get Smart gadgets connected to the network provide real-time information. Acknowledgement and key configuration between an authorized user and an accessible intelligent industrial gadget must be transported out via an important intermediate node known as the content server, which is positioned between the two parties, in order to reduce these problems.. Thus, it is necessary to develop a unique and robust "user authentication and key agreement system" for mutual authentication and key setup between users and intelligent industrial devices through the server of content Problem Statement

Most of the applications used in the 6G-enabled NIB are not appropriately secured. There are chances of several active and passive attacks due to the insecure channel. An authentication scheme (UAKMS-NIB) is presented in the Wazid et al. article. However, there is a missing step to exchange the authentication key between the content server and smart devices. The smart device sends the key directly to the user without having any information about the authentication key. Therefore, it is not possible to communicate without the exchange of authentication key information.

1.4. Contributions

To counter the above-mentioned incorrectness, this thesis proposes an improved scheme based on elliptic curve, which provides user authentication and better security.

The significant contributions of this thesis are as follows:

- • The iUAKMS-NIB is a new enhanced remote user authentication mechanism enabling secure connection in 6G-capable NIBs used in industrial uses. It is the first time that this technique has been suggested. After authenticating a smart industrial device with the iUAKMS-NIB, a confirmed user may access the device's real-time data using the establish session key that was generated after authenticating the device.
- It was done in this thesis utilizing the widely recognized program ProVerif, which is used to automatically analyze the security of cryptographic protocols. It also included formal security verification. A number of conceivable assaults on the iUAKMS-NIB are proved to be robust in a 6G-enabled NIB environment, which is necessary in this study.
- Finally, a comprehensive comparison research between the updated iUAKMS-NIB and UAKMS-NIB The comparison of several user authentication techniques demonstrates that the efficiency of of iUAKMS-NIB is superior to the performance of other existing competing schemes in terms of user authentication.

1.5. Thesis Organization

Chapter two provides an overview of the current schemes that are related to the topic. Chapter Three provides an explanation of the System Model that consists of Network Model and Threat Models. Chapter Four explains Wazid et al. scheme, its Pitfalls and the proposed scheme. The Performance analysis such as Computational Cost and Communication Cost are performed in Chapter Five. Chapter Five also explains a security analysis of the proposed scheme by employing BAN logic. The thesis concluded in Chapter Six.

CHAPTER TWO

BACKGROUND STUDIES

2.1. 6G Technologies and Applications

By 2030, the digital society will have a significant impact on our daily lives. We'll start with gadgets that people may utilize to connect to the network as a starting point. While the smartphone and the tablet will continue to exist, it is likely to witness the introduction of new man-machine interfaces that will make it far more comfortable for us to consume and manipulate information going forward. Following are the main points to be observed in the future 6G technologies, and shown in Figure 1.

1) Wearable technologies such as earphones and electronics integrated in our clothes will become popular, and skin patches and bio-implants will likely become commonplace as well. Everyone will rely on new brain sensors to control robots in the future. We will have a number of wearables that will be carried and users will communicate with one another smoothly, giving natural and intuitive interfaces. The future development of technologies is shown in Figure 2.
2) It is conceivable that touch-screen typing will become obsolete.
3) The gadgets will be completely context-aware, and the network will grow cleverer at anticipating our demands. Context awareness, in conjunction

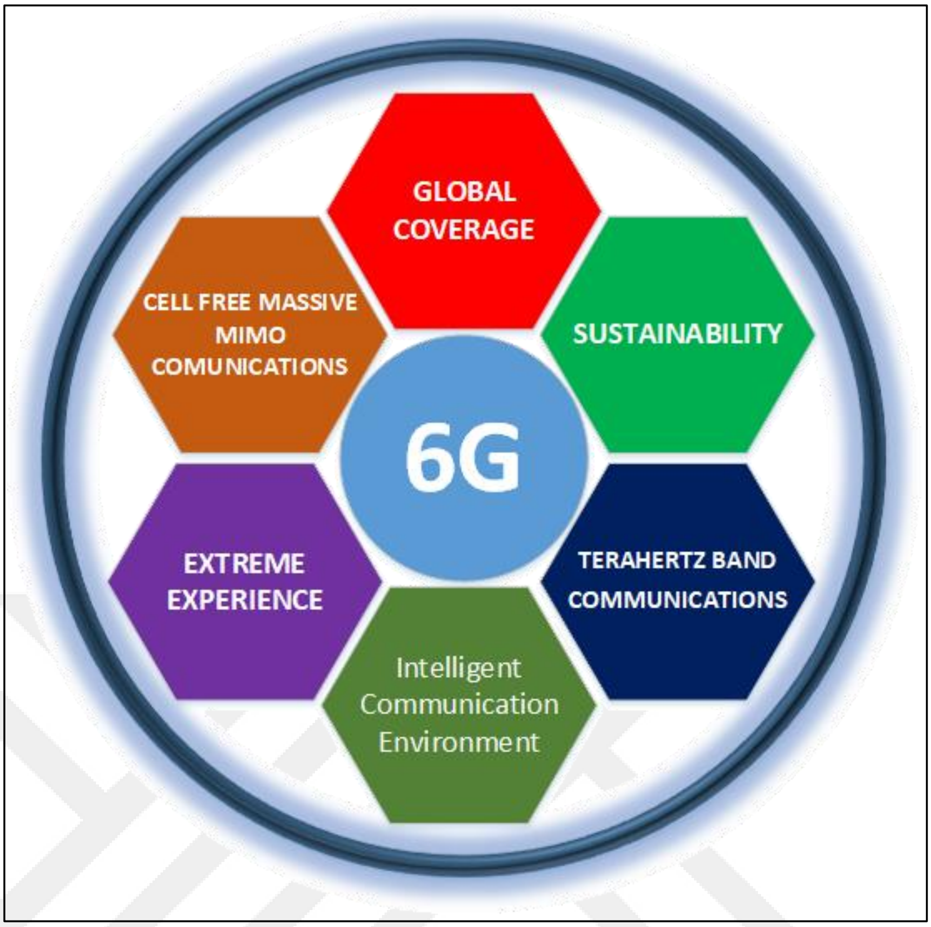
GLOBAL COVERAGE
CELL FREE MASSIVE MIMO COMUNICATIONS
SUSTAINABILITY
6G
EXTREME EXPERIENCE
TERAHERTZ BAND COMMUNICATIONS
Intelligent Communication Environment

Figure 1: 6G Technologies and Applications

4) with new human-machine interfaces, will make our interaction with the real and digital worlds much more intuitive and efficient in the near future.

Because of form design and battery capacity constraints, it is probable that not all of the computation required for these devices will be housed inside the devices themselves. As a result, they may be forced to depend on locally available computer resources to execute activities that are not compatible with the edge cloud. As a result, networks will play an important role in the future of the human-machine interface (HMI).

According to current research autonomous vehicles will be available to the general public by the 2030s. Although they will most likely be self-driving, they will almost surely need the aid of a remote driver or a passenger in order to take control in certain scenarios. Because of this, the system will have substantially more time to absorb information from the internet, whether it be more enjoyment, more in-depth chats with others, or more educational stuff. Additionally, since vehicle sensor data will be sent in real time to the network, high-resolution maps will be downloaded, and cars will be able to speak with one another directly via the network, the vehicles themselves will use a significant amount of data. The following considerations are expected in the future 6G technologies.

1) Using wireless cameras as sensors will become much more common, according to predictions. AI and machine vision improvements, together with their capacity to detect people and things (or, more broadly to automatically collect information from photos and videos), will convert the camera into a universal sensor that can be utilized nearly everywhere in the globe. In order to address privacy concerns, access to data will be limited, and information will be anonymized as much as possible. It also employs radio frequency technology and other sensing modalities.
2) Acoustics, for example, will be used to gather information about the surrounding environment and its inhabitants. Advanced technology will be used in security-screening processes in order to reduce the need for lengthy security lines at the airport, which will benefit passengers. Individuals will be screened as they pass through highly populated areas rather than simply as they arrive at checkpoints, using a combination of numerous sensing modalities rather than just one. The use of radio sensing, which will be enabled by future communication systems, will be a significant component of this endeavour.
3) If digital money and keys become the norm, it is feasible that transactions could occur in both the physical and digital worlds via the range of devices that can be useful in the future.
4) In order for such a change to be conceivable, the network of the future must provide the necessary levels of security and privacy. A flurry of home service robots will be released in the next years to complement the vacuum cleaners and lawn mowers. Perhaps they will take the form of a horde of smaller robots that will work together to execute tasks in a collaborative manner. The robots will be equipped with video cameras that will stream live video to a local computer server where it will be processed and analyzed in real time. Because of this, the number of devices linked to our

home networks will expand, as will the amount of bandwidth necessary to support those devices.

5) Because of the growing usage of wearable devices to continuously monitor important parameters in both healthy and unwell people, health care will experience a dramatic transition as a consequence of their broad adoption and use. The use of in-body devices to interact with wearables outside the body, which will thereafter be able to communicate the data to the internet, is also envisaged in the future of health monitoring. Before the year 2030, the shift to Industry 4.0 will have been place, as will the deployment of the first wave of wirelessly linked automation. Because of the availability of 5G networks, which allow ultra-reliable, low-latency connections, it will be feasible to do real-time processing in the cloud in the near future (URLLC). While 5G would be sufficient for most consumer applications, 6G will be necessary for industrial applications that have even stricter criteria for wireless communication.
6) It is expected that holographic telepresence will become the norm for both business and social interaction in the not-too- distant future. It will be possible to provide the appearance that one is in one area while really being in another location, for example, looking to be in the city while actually being in the countryside, if the technology is developed.
7) While really driving to work, you may pretend to be in the office. The digital portrayal of any genuine reality will include technologies that merge current facial expressions with a virtual self that is formed in real time, allow the users to see themselves in reality. In a range of businesses, such as hotels, hospitals, warehouses, and package delivery, mobile robot swarms and autonomous drones will be extensively deployed. If it is continued to enhance human intelligence, it will be vital to create dynamic digital twins in the digital domain that are more exact and synchronized in their updates of the physical world.

In light of the above view of the future, it might infer the following essential use cases. The new 6G technologies allow a mix of what 5G will offer, but with widespread adoption occurring in the period of 6G utilizing new technologies, as well as a new set of use cases that are made possible by the new 6G technologies.

2.2. 6G Requirements and Key Performance Measurements

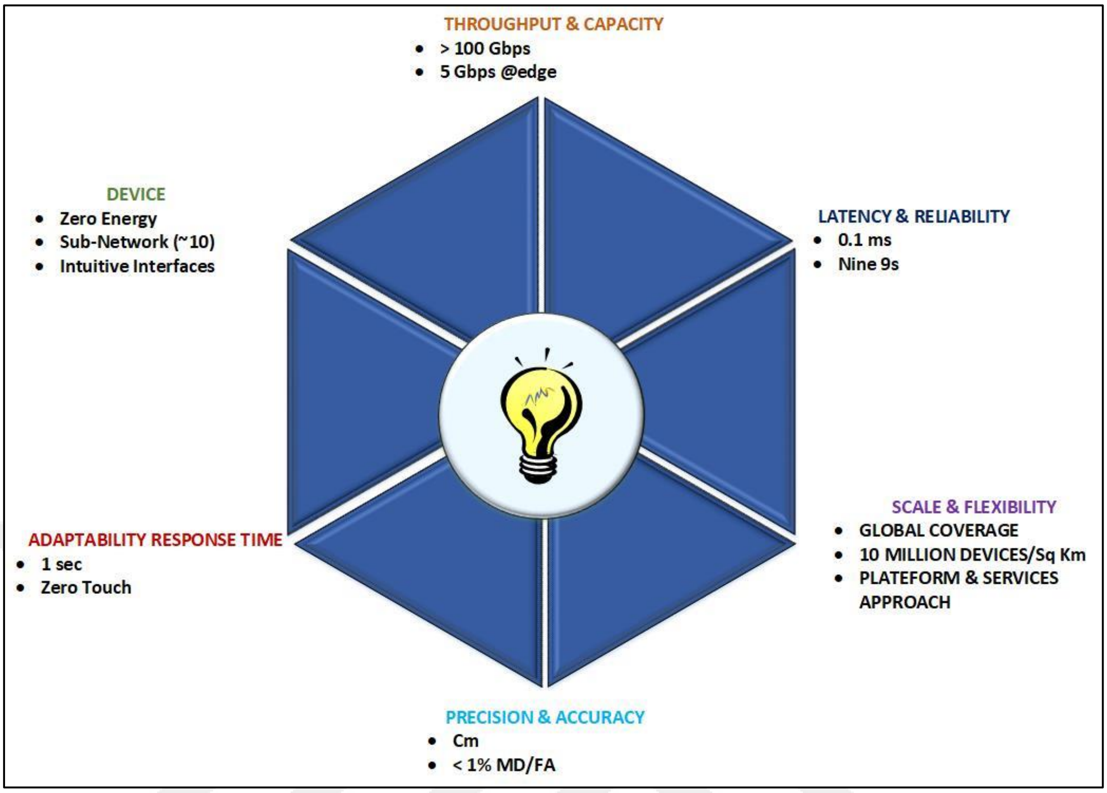

Figure 2: Key requirements and characteristics of 6G

The multiplicity of new use cases expected by 2030 and beyond will serve as the driving force behind the extra requirements that must be satisfied by 6G in order for it to be implemented. When evaluating 6G performance, it will be critical to use the same key performance indicators (KPIs) that were used to evaluate 5G performance, such as data rate and throughput, capacity and latency, reliability, scalability and flexibility, among other things. Following the discussion of the anticipated use cases outlined in the previous section, many new characteristics will become important for 6G networks in the future. The Figure 2 represents the the key requirements and charactristics along with their KPIs of 6G mobile networks. It is also shown some of the categories with KPIs similar to those for 5G. One of the most important features of 6G will be the capacity to identify and feel items over a communication network.

To compare the performance of localization and sensing systems, precision and accuracy as performance indicators are employed in this thesis. As a result, it is estimated that the precision of this work will be on the millimetre level. The accuracy of object sensing may be measured in terms of the likelihood of missed detection (MD) and false alarm (FA), as well as the inaccuracy in parameter estimation.

Second, the network will be developed with distributed AI and machine learning techniques implanted in various nodes, and the speed with which they adapt to changing network conditions will be a significant performance indicator in the network's development. It will become standard practice to automate networks, and the degree to which networks are automated to the point where no human interaction is necessary will be a consideration in determining which networks to purchase and which networks to avoid.

At last but not the least, It is foreseen a significant transformation in the end device throughout the era of the 6G network deployment. As a result, a few features under each device category in order to draw attention to the important alterations are provided. Therefore, It will take place in the near future. In the first place, It is believed that in many cases, the end device will expand to become a network of devices or a sub-network of devices. As an example, consider a machine-area network or a robot-area network, which are both types of networks that connect various elements of a machine, such as a controller and its drives, to one another. Using gestures rather than typing, for example, will allow the users to access information on our devices in the 6G age, which will be another differentiating characteristic. The last option for a specialized device class will be extremely low-power and maybe battery-less, with the device relying on the network to deliver the necessary power.

2.3. Related Work

The (Pozza et al., 2018) provided various cases that inspired the creation of the NIB idea. The common aspects of NIB implementations, as well as other ideas, were addressed. Some of the potential study avenues that may be pursued were also mentioned.

The (Ramaswamy & Correia, 2018) presented a variety of approaches for improving the robustness of Long-Term Evolution (LTE) networks that are used for military and public safety operations. It is possible that these approaches will be enabled via the Third Generation Partnership Project (3GPP) LTE standards and that they will also be deployed as software enhancements for existing systems.

A management strategy proposed by (Thyagaturu et al., 2016) allowed a large number of operators, for example, multiple Servicing/Packet Gateways (S/P GWs), to operate dynamically via multiple Smart Gateways (Sm-GWs) in a large number of micro cells using a single Smart Gateway (Sm-GW). The Sm-GWs, which were based on Software-Defined Networking (SDN), were in charge of coordinating the adaptive allocation of uplink transmission bit rates to evolved NodeBs (eNBs) in response to changing requirements. The (Ramaswamy & Correia, 2018) presented a variety of approaches for improving the robustness of LTE networks that are used for military and public safety operations. It is possible that these approaches will be enabled via the 3GPP LTE standards and that they will also be deployed as software enhancements for existing systems.

A management approach developed by (Thyagaturu et al., 2016) enabled numerous drivers (for ex - ample, multiple Servicing/Packet Portals (S/P GWs) in order to work dynamically via many Sm-GWs in a large number of tiny cells) to operate in a dynamic manner through multiple Sm-GWs in a large number of tiny cells It is the Smart gateways (Sm-GWs) based on Software-Defined Networking (SDN) that are in charge of coordinating the adaptive distribution of up . this is probably bit rates to evolved NodeBS (eNB) in accordance with the demands of each node.

The authors of (Sizer et al., 2021) discussed the significant technological breakthroughs that might be used to power the 6G mobile network. This includes topics like "conceptual bandwidth able to share methods for latest available spectrum," "connectivity of localization and sensor technologies" into a system's description, "achieving maximum performance demands in order of latency," new connectivity concepts such as "sub-networks" and "RAN-Core integration," advanced data security techniques, amongst others. On the other hand, (Yang et al., 2020) identified certain probable requirements and provided an overview of the most recent research on viable ways for developing 6G, which has garnered substantial interest. In addition, the major technological issues related with 6G, as well as possible solutions, were examined at length.

Samdanis and colleagues (Samdanis & Taleb, 2020) provided an overview of key technologies that will serve the development of "mini core networks, native IP-based user planes, network analytics," and "help for low delay reliability" as foundations of the growth of wireless connectivity beyond 5G They focused on "micro-service-oriented core networks," "native IP-based user planes," "network analytics," and "support for low latency-high reliability." It was also examined what problems remain in terms of technical and business requirements, such as building "softwarization footprints," "security and trust," and " a discussion of "distributed architectures and services" in the context of 6G deployments, and how to overcome the challenges.

CHAPTER THREE

SYSTEM MODEL

The proposed scheme i.e., iUAKMS-NIB is explained by using the following two models. The overall system model is given in the Figure 3.

3.1. Network Model

Figure 3 depicts the network model of the "6G-enabled Network in a Box (NIB)" that has been implemented for industrial applications. NIB provides the connections and enables the various sorts of entities to communicate with each other. It is used to provide integrated voice and data services via mobile communication networks such as 3G and 4G, and beyond mobile networks. The EPC incorporates critical components such as the Packet Data Network Gateway (P-GW), the Serving Gateway (S-GW), the Mobility Management Entity (MME), and the home subscriber server, to name a few Home Subscriber Server (HSS). The mobile device serves as a connection point between external networks. It serves as the point of entry for data flow for a mobile device's user. The mobile device of the user may be connected to many P-GWs at the same time in order to get access to multiple P-GWs. Furthermore, SGW is in charge of the routing and forwarding of user data packets on behalf of the network. Among other things, it is in charge of inter-eNB handovers and the provision of mobility between LTE and other types of networks (for example, between 2G/3G and P-GW), among other things as well. An evolebed Node Basestation (eNB) is a base station that has been upgraded and is responsible for regulating the mobile phones in a group of cells. As its name implies, the serving eNB is the base station that establishes communication between the user's mobile device and the network. In the NIBThe MME is involved in a number of activities, for example "idle mode user's smart phone tracking," "paging method (i.e. retransmissions)," "bearer authentication and disablement process," "S-GW selection for a user's mobile device at the initial attach," "within- with Data Centre," and "user's smart phone verification with HSS." Aside from that, the MME server is responsible for ciphering and integrity protection for Non-Access Stratum (NAS) signaling, in addition to security key management. The HSS system is also an important component of the NIB system. One node in the cluster is dedicated to the maintenance of the master user database. (i.e., a piece of

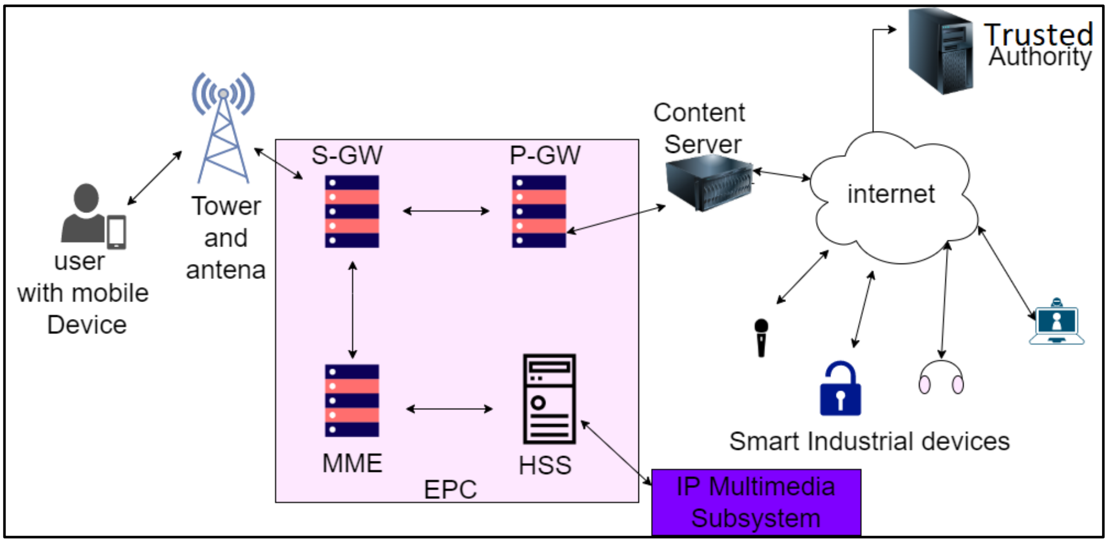

Figure 3: 6G enabled NIB System Model

equipment). Consumers may be managed by suppliers of phone services in timely manner and at a price that is affordable. as a result of this technology. Among other things, the HSS database stores information on subscribers (also known as users) in order to aid in the authorization process. This information includes characteristics about the devices used, among other things, the device's position and other application information are collected. The IP multimedia subsystem receives the user's request and connects it to the IP multimedia subsystem (IMS). An IMS (Integrated Management System) is a critical The Internet Protocol (IP) is an important part of an overall system of telecom operators because it allows the use of IP (Internet Protocol) for a variety of types of data packets in wired or wireless connectivity, such as phones, mail, e-mail, High speed internet, online services, and videoconferencing (VoIP), among other things, in a web of telecom service providers that is integrated. Additionally, the content server, which acts as a connection between users and smart industrial equipment, is a critical node in the network's architecture.

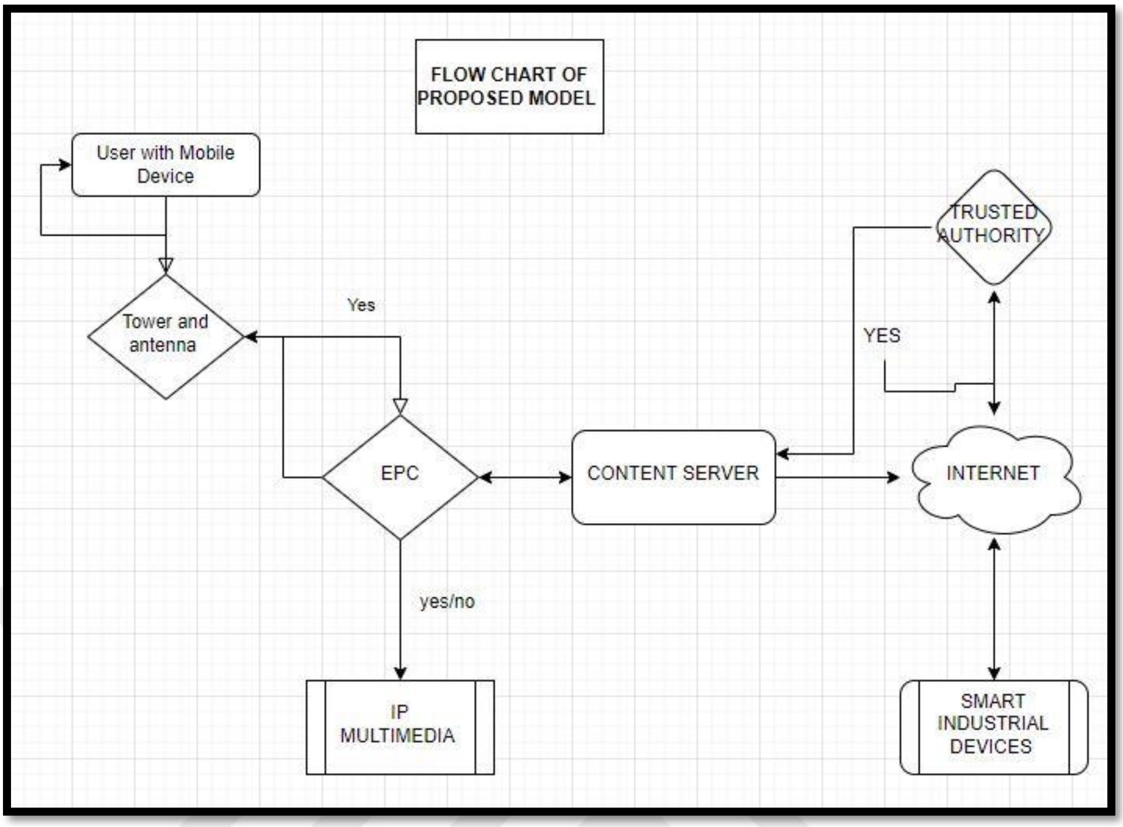

Figure 4: Flow Chart of Proposed Model

A smart industrial device network has been built on this network for the purpose of monitoring and controlling industrial machinery. Each intelligent industrial gadget has a certain goal in mind that it strives to achieve. Users of an industrial facility may sometimes be interested in gaining access to real-time data collected by smart industrial equipment. Users and smart industrial equipment must go through the procedures of authentication and key setup methods in order to be able to share information in a safe manner with one another.

3.2. Threat Model

During the development of iUAKMS-NIB, the famose "Dolev-Yao threat model is considered (Ram & Odelu, 2022), which is as well known as the DY model, shown in Figure 4. The communicative entities (parties) speak with one another over an open channel as a result. Individuals who interact with the end-point entities (such as users and smart industrial equipment) are not often regarded as trustworthy. The trustworthy authorities (TA) of the "6-Genabled NIB deployed for commercial

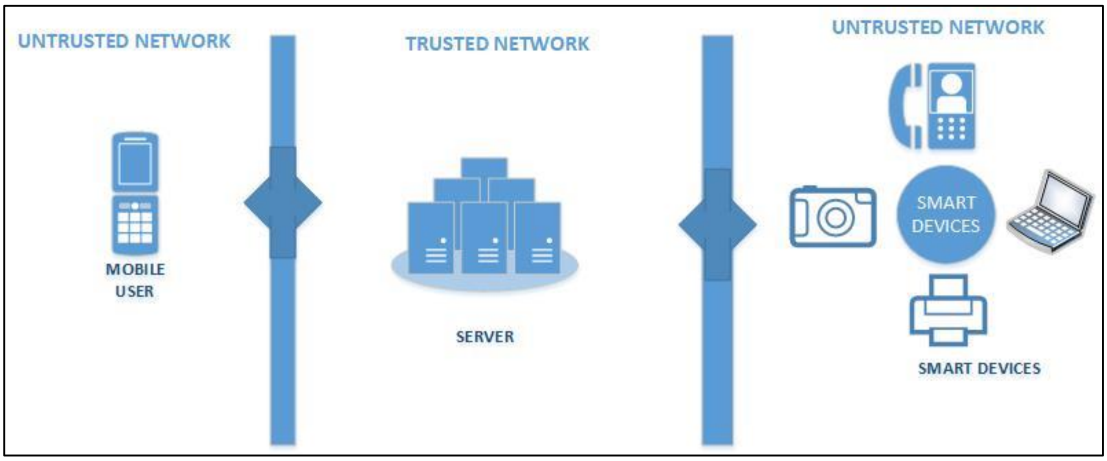

Figure 5: The overall Threat Model used in 6G-NIB

applications" is, on the other hand, regarded to be the completely trusted node. In any event, the TA should not be infiltrated since it is responsible for the registration of organizations inside the network (including users, content servers, and smart industrial devices). If the TA is hacked, If this were to happen, the safety of the whole system would be compromised. Aside from just that, the media server in the network could be considered a trustworthy entity by certain users. Furthermore, it is believed that the memory unit of the user's mobile device (MD) is not provided with tamper-resistant capabilities to prevent unauthorized access. By using power analysis techniques, a hacker may hijack a user's mobile device and retrieve all of the sensitive information that has been saved on it from the device's memory (Abdel Hakeem et al., 2022).

A model known as the "CK-adversary model"(Mookherji et al., 2022) , which is now de facto standard in the design of key exchange systems, is also taken into consideration in iUAKMS-NIB. According to this example, A may tamper with messages in the same way as he or she can in the DY model, Other than altering messages, he or she could also compromise session keys, private keys, and other session states via session hijacking attacks, which are similar to middle attack assaults in that they expose shared key, private keys, and other process states.

CHAPTER FOUR

THE WAZID ET AT.’S UAKMS-NIB SCHEME

This section explains the Wazid et al. scheme named as UAKMS-NIB. Different phases used in UAKMS-NIB schemes are discussed in details. The symbols and their explainations are givne in Table 1.

Table 1. Symbols and Explanation

Symbol	Explanation
$\boldsymbol{A}$	An adversary
$\boldsymbol{U_x}$, $\boldsymbol{D_x}$	x^{th} user with his or her cell phone
$\boldsymbol{ID_x}$, $\boldsymbol{RD_x}$	x’s identity and pseudo identity, respectively
$\boldsymbol{PW'_x}$, $\boldsymbol{BO_x}$	x’s password and biometric, respectively
$\boldsymbol{TA}$, $\boldsymbol{ID_{TA}}$	Identified trusted authority
$\boldsymbol{RD_{TA}}$	TA’s pseudo identity
$\boldsymbol{CS_y}$,$\boldsymbol{ID_y}$	y^{th} a content server's identity
$\boldsymbol{RD_y}$	Pseudo identity of content server
$\boldsymbol{SD_z}$, $\boldsymbol{ID_z}$	y^{th} A smart industrial device identity,
$\boldsymbol{RD_z}$	Pseudo identity of SD_z
$\boldsymbol{d_x}$, $\boldsymbol{d_y}$	160-bit secret keys of U_x and CS_y respectively
$\boldsymbol{d_z}$, $\boldsymbol{d_{TA}}$	Secret keys of SD_z and TA, respectively
$\boldsymbol{X}$	1024-bit long-term random secret of U_x
$\boldsymbol{r_x}$, $\boldsymbol{r_y}$	160-bit weird secrets of U_x and CS_y,

$\boldsymbol{r_z}$	160-bit random secret of SD_z
$\boldsymbol{T_s}$	Different timestamps
$\boldsymbol{\Delta T}$	highest delay in transmission
$\boldsymbol{Gen}(\cdot)$	Method of generating in fuzzy extractor
$\boldsymbol{Rep}(\cdot)$	Mechanism of replication in fuzzy extractor
$\boldsymbol{\alpha'_x}$	Biometric secret key of U_x for BO_i
$\boldsymbol{\tau_x}$	Public reproduction parameter of U_x for BO_x
$\boldsymbol{t}$	Fuzzy extractor needs a certain level of error tolerance.
$\boldsymbol{h}(\cdot)$	Collision-resistant cryptographic one-way hash function
$\boldsymbol{SK_x, SD_z}$	Session key between U_x and SD_x
$\|\|,\oplus$	Concatenation and the bitwise XOR operation,
$\boldsymbol{d_e}$	The secret key of entity E
$\boldsymbol{Q_e}$	Public key of entity E, where $Q_e = d_e \cdot P$, where P is an elliptic curve point.

4.1. Registration Phase

This phase is executed by a trusted authority (TA) and for this TA select an elliptic cure $E_p(x_x, x_y): y^2 = x^3 + x_x + x_y(modp)$ and a base point P over $GF(p)$. The TA then selects a oneway hash function $h(\cdot)$.

4.1.1. Smart Industrial Device Registration

The TA registers the Smart Industrial Device (SD_z) through execution of following steps:

(i) The TA selects it's own secret key d_{TA} and the identity, secret key and public key tuple $\{ID_z, d_z, Q_z = d_z \cdot P\}$ for SD_z along with pseudo identity $RD_z = h(ID_z \parallel d_{TA})$. The TA then using the timestamp RTS_z, computes $TC_z = h(d_z \parallel ID_z \parallel RTS_z \parallel d_{TA}$.

(ii) The information obtained from RD-1, such that RD_z, TC_z, Q_z, d_z, $h(\cdot)$, $E_p(a,b)$, P is stored in the memory of SD_z. It is noted that Q_z is announced widely to the other entities. In addition, RD_z can be sent to CS_y by TA in a secure way.

4.1.2. Content Server Registration

The content server CS_y is registered during this phase. This task is executed by TA in the following steps.

(i) In order to calculate the pseudo-identity of CS_y as $RD_y = h(ID_y \parallel d_{TA})$, public key $Q_y = d_y \cdot P$, the TA picks a particular identity ID_{CSj} as well as a secret key chosen at random d_y for CS_y. Meanwhile, it also generates it own pseudo random identity $RD_{TA} = h(ID_{TA} \parallel d_{TA})$.

(ii) The related content server and user information RD_y, RD_x, TID_x, RD_{TA}, RD_z, Q_y, d_y, $h(\cdot)$, $E_p(a,b)$, P is stored on a database created over a temper resistant memory pf the TA. Here, $\{RD_x, TID_x\}$ are registered user (U_x) related parameters. The public key Q_y of the content server is publicly available to all intended entities.

4.1.3. User Registration

This phase furnishes the user registration.The registration curious user U_x and TA mutually communicate over a secure channel through execution of following steps to accomplish this phase:

(i) The U_x selects identity-password pair $\{ID_x, PW'_x\}$ in addition to a secret and random long term key $x \epsilon Z_p^*$, and then it computes $RPW'_x = h(PW'_x \parallel x)$. Now, U_x transmits $\{ID_x, RPW'_x\}$ to TA.

(ii) On receiving $\{ID_x, RPW'_x\}$, the TA computes pseudo and temporary identity pair $\{RD_x = h(ID_x \parallel d_{TA}), TID_x\}$, in addition to a secret and random key $d_x \epsilon Z_p^*$. After then, the TA computes $Q_x = d_x \cdot P$, the public key for the U_x and the temporary parameters The TA computes temporal credential of U_x as $TC_x = h(ID_x \parallel RPW'_x \parallel d_x \parallel d_{TA} \parallel RTS_x)$ and $\alpha'_x = h(RPW'_x \parallel RD_x) \oplus d_x$ (also termed as temporal credentials) for U_x. The TA now sends the tuple containing $\{RD_x$, TID_x, RD_{TA}, TC_x, α'_x, Q_x, $h(\cdot)$, $E_p(a,b)$, $P\}$ to U_x. The TA places Q_x over a public space and any intended identity has access to the Q_x.

(iii) On receiving $\{RD_x$, TID_x, RD_{TA}, TC_x, α'_x, Q_x, $h(\cdot)$, $E_p(a,b)$, $P\}$, The U_x pins BO_x and the D_x computes $(\alpha'_x, \tau_x) = GenB(BO_x)$, where BO_x, α'_x and τ_x are the U_x's biometrics information, BO_x related secret key and re-production parameter, respectively. Moreover, the "$GenB(\cdot)/RepB(\cdot)$ are generation and re-production functions of the fuzzy-extractor related to the biometrics. Now the U_x further computes $d_x = h(RPW'_x \parallel RD_x) \oplus \alpha'_{U_x}$, $TC_x = h(TC_x \parallel x \parallel \alpha'_x)$, $x^* = x \oplus h(ID_x \parallel PW'_x \alpha'_x)$, $RD_x^* = RD_x \oplus h(PW'_x \parallel \alpha'_x)$, $TID_x^* = TID_x \oplus h(ID_x \parallel PW'_x)$, $RD_{TA}^* = RD_{TA} \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$, $TC_x^* = TC_x \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x$, $d_x^* = d_x \oplus h(ID_x \parallel \alpha'_x)$ and $LV = h(ID_x \parallel RPW'_x \parallel TC_x \parallel d_x \parallel \alpha'_x)$. The U_x then updates the D_x with the tuple RID_x^*,TID_x^*, RD_{TA}^*, TC_x^*, d_x^*,Q_x, τ_x, LVx^*, $h(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, t, $E_p(a,b)$, P.

The TA on successful registration of a user U_x communicates RD_x, TID_x to CS_y and it removes the tuple RD_x, TID_x, RD_y, RD_z, d_x, d_y, d_z, TC_x, TC_z, α'_x, RPW'_x from TA's own memory.

4.2. User Login and Authentication Phase

A registered user U_x initiates this step to get NIB services and for this the U_x performs following login and authentication steps:

The U_x submits the tuple $\{ID_x, PW'_x, BO'_x\}$ consisting of it's identity, password and biometrics. The D_x checks the relation of BO'_x with the user-biometrics imprinted during registration phase and in case if both biometrics match each other the D_x computes $\alpha'_x = RepB(BO'_x,\ \tau_x)$. Now, the user side computes $x = x \oplus h(ID_x \parallel PW'_x\alpha'_x), RPW'_x = h(PW'_x \parallel x), RD_x = RD_x \oplus h(PW'_x \parallel \alpha'_x), TID_x = TID_x \oplus h(ID_x \parallel PW'_x)$, $RD_{TA} = RD_{TA} \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$, $TC_x = TC_x \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$, and $\alpha' d_x = d_x \oplus h(ID_x \parallel \alpha'_x)$. Now D_x confirms the authenticity of U_x if $LV \overset{?}{=} h(ID_x) \parallel RPW'_x \parallel TC_x \parallel d_x \parallel \alpha'_x)$ holds and furthers the process by generating the timestamp and random number pair $\{T_1, r_x\}$. The user device now computes $M_1 = h(r_x \parallel T_1) \oplus (RD_{TA} \parallel RD_x \parallel d_x \cdot Q_y \parallel T_1), MM_1 = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1), M_x = h(RD_x) \parallel\ M_2 = M_x \cdot P,\ M_3 = M_x + h(r_x \parallel T_1) \cdot d_x$ and selects the smart device with RD_z as it's pseudo identity. U_x completes this step by sending $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$ to CS_y via open channel.

After successful login and receiving of $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$, the CS_y after confirming the timestamp (T_1) freshness extracts RD_x relevant to the received TID_x. The CS_y then computes $h(r_x \parallel T_1) = M_1 \oplus h(RD_{TA} \parallel RD_x \parallel d_y \cdot Q_x \parallel T_1)$ and $M_x = h(RD_x \parallel RD_{TA})$. The CS_y confirms the genuineness of the U_x if $M_3 \cdot P \overset{?}{=} M_2 + h(r_x \parallel T_1) \cdot Q_x$. The CS_y after confirming genuineness generates timestamp and random number pair $\{T_2, r_y\}$ and computes $M_4 = h(r_y \parallel T_2 \parallel RD_y) \oplus h(RD_z \parallel d_y \cdot Q_z \parallel T_2)$, $MM_2 = MM_1 \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$, $M_y = h(RD_z \parallel T_2)$, $M_5 = M_z \cdot P$ and $M_6 = M_y + h(r_y \parallel T_2 \parallel RD_y) \cdot d_y$. The CS_y then generates TID_x^{new}, and computes $M_T = TID_x^{new} \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_2)$, where TID_x^{new} is the new temporary identity for U_x. Now, the CS_y sends $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$ to SD_z.

On receiving $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$, the SD_z after confirming the timestamp (T_2) freshness, computes $h(r_y \parallel T_2 \parallel RD_y) = M_4 \oplus h(RD_z \parallel d_z \cdot Q_y \parallel T_2), h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) = MM_2 \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$, $M_y = h(RD_z \parallel T_2)$ and checks $M_6 \cdot P \overset{?}{=} M_5 + h(r_y \parallel T_2 \parallel RD_y) \cdot Q_y$. The SD_z further computes $X_s = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA})$, if the previous condition holds. The SD_z furthers the process by generating the timestamp and random number pair $\{T_3, r_z\}$ and computes $M_7 = h(r_z \parallel T_3) \oplus h(T_1 \parallel T_3 \parallel d_z \cdot Q_x)$, $M_x = h(RD_z \parallel TC_z) \oplus h(h(r_z \parallel T_3) \parallel T_1)$, $M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$, $M_8 = M_z \cdot P$, and the session key $SK_{SD_z,U_x} = h(X_s \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$. The SD_z now generates signatures $M_9 = M_z + h(SK_z,\ U_x \parallel M_T \parallel T_1 \parallel T_3) \cdot d_z$ and sends $M_{sg3} = \{M_7, M_x, M_8, M_9, M_T, T_3, T_2\}$ to U_x.

On receiving $M_{sg3} = \{M_7, M_x, M_8, M_9, M_T, T_3, T_2\}$, the U_x after confirming the timestamp (T_3) freshness, computes $h(r_z \parallel T_3) = M_7 \oplus h(T_1 \parallel T_3 \parallel Q_z \cdot d_x)$, $h(RD_z \parallel TC_z) = Mx \oplus h(h(r_z \parallel T_3) \parallel T_1)$, $M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$ and session key $SK_{U_x,SD_z} = h(h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$. Now, U_x verifies the genuineness of the SD_z by verifying the equality $M_9 \cdot P \overset{?}{=} M_8 + h(SK_{U_x,SD_z} \parallel M_T \parallel T_1 \parallel T_3) \cdot Q_z$ and on successful verification, the U_x computes $TID_x^{new} = M_T \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_2)$ and replaces TID_x by TID_x^{new}.

Table 2. Wazid et al.'s Scheme

User (U_x) / Mobile Device (D_x)	Content Server (CS_y)	Smart Industrial Device (SD_z)
Submit ID_x, PW'_x, BO'_x Computes $\alpha'_x = Rep(BO'_x, \tau'_x)$ $x = x^* \oplus h(ID_x \parallel PW'_x \parallel \alpha'_x) RPW'_x = h(PW'_x \parallel x)$ $RD'_x = RD_x^* \oplus h(PW'_x \parallel \alpha'_x)$ $TID'_x = TID_x^* \oplus h(ID_x \parallel PW'_x)$ $RD'_{TA} = RD_{TA}^* \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$ $TC'_x = TC_x^* \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$ $d_x = d_x^* \oplus h(ID_x \parallel \alpha'_x)$ Check $LV' \overset{?}{=} h(ID_x) \parallel RPW'_x \parallel TC'_x \parallel d_x \parallel \alpha'_x)$ Generate T_1, $r_x \epsilon Z_p^*$ & Compute		

$M_1 = h(r_x \parallel T_1) \oplus h(RD_{TA} \parallel RD_x \parallel d_x \cdot Q_y \parallel T_1)$ $MM_1 = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1)$ $M_x = h(RD_x) \parallel RD_{TA})$ $M_2 = M_x \cdot P$ $M_3 = M_x + h(r_x \parallel T_1) \cdot d_x(\text{mod } p)$ $\xrightarrow{M_{sg1}=\{TID_x,RD_z,M_1,MM_1,M_2,M_3,T_1\}}$		
	Verifies T_1 Fetch RD_x and compute $h(r_x \parallel T_1) = M_1 \oplus h(RD_{TA} \parallel RD_x \parallel d_y \cdot Q_x \parallel T_1)$ $M_x = h(RD_x \parallel RD_{TA})$ Check $M_3 \cdot P \overset{?}{=} M_2 + h(r_x \parallel T_1) \cdot Q_x$ Generate T_2, $r_y \epsilon Z_p^*$ & Compute $M_4 = h(r_y \parallel T_2 \parallel RD_y) \oplus h(RD_z \parallel d_y \cdot Q_z \parallel T_2)$ $MM_2 = MM_1 \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$ $M_y = h(RD_z \parallel T_2)$ $M_5 = M_z \cdot P$ $M_6 = M_y + h(r_y \parallel T_2 \parallel RD_y) \cdot d_y$ Generate TID_x^{new} and Compute $M_T = TID_x^{new} \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_2)$ $\xrightarrow{M_{sg2}=\{RD_z,M_4,MM_2,M_5,M_6,M_T,T_1,T_2\}}$	
		Verify T_2 & Compute

		$h(r_y \parallel T_2 \parallel RD_y) = M_4 \oplus h(RD_z \parallel d_z \cdot Q_y \parallel T_2)$ $h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) = MM_2 \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$ $M_y = h(RD_z \parallel T_2)$ Check $M_6 \cdot P \overset{?}{=} M_5 + h(r_y \parallel T_2 \parallel RD_y) \cdot Q_y$ $X_s = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA})$ Generate T_3, $r_z \epsilon Z_p^*$ & Compute $M_7 = h(r_z \parallel T_3) \oplus h(T_1 \parallel T_3 \parallel d_z \cdot Q_x)$ $M_x = h(RD_z \parallel TC_z) \oplus h(h(r_z \parallel T_3) \parallel T_1)$ $M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$ $M_8 = M_z \cdot P$ SK_z, $U_x = h(X_s \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$ $M_9 = M_z + h(SK_{z,x} \parallel M_T \parallel T_1 \parallel T_3) \cdot d_z$ $\xleftarrow{M_{sg3}=\{M_7,M_x,M_8,M_9,M_T,T_2,T_3\}}$
Verifies T_3 and Compute $h(r_z \parallel T_3) = M_7 \oplus h(T_1 \parallel T_3 \parallel Q_z \cdot d_x)$ $h(RD_z \parallel TC_z) = Mx \oplus h(h(r_z \parallel T_3) \parallel T_1)$ $M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$		

$SK_{x,z} = h(h(h(r_x \parallel T_1)$ $\parallel TC_x \parallel T_1$ $\parallel RD_x$ $\parallel RD_{TA})$ $\parallel h(r_z \parallel T_3)$ $\parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$ $M_9 \cdot P \overset{?}{=} M_8 + h(SK_{x,z} \parallel M_T$ $\parallel T_1$ $\parallel T_3) \cdot Q_z$ $TID_x^{new} = M_T \oplus h(h(r_x$ $\parallel T_1)$ $\parallel RD_{TA}$ $\parallel TID_x \parallel T_2)$ Replace TID_x with TID_x^{new}		

4.3. Pitfalls of Wazid et al.'s Scheme

In this section, it is proved that the Wazid et al.'s scheme can not provide authentication among a user and a smart device. Moreover, it is also shown that their scheme entails identity de-synchronization issues.

4.3.1. Incorrectness

The authentication phase of Wazid et al.'s scheme is incorrect and it cannot be completed. As a severe consequence, the user and the smart industrial device may not share the key at all. Precisely, a user initiates a request by computing and sending $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$ to CS_y and the CS_y further processes the request and after verifying the legitimacy of the the user say U_x, direct message $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, M_T, T_1, T_2\}$ to SD_z. The SD_z processes the message and verifies the legitimacy of CS_y, After then SD_z computes and sends $M_{sg3} = \{M_7, M_x, M_8, M_9, M_T T_3, T_2\}$ to U_x. In this whole process the SD_z does not verify the legitimacy of the user U_x rather SD_z does not know the real or pseudo identity of the user U_x and the message M_{sg2} received from CS_y also does not contain any tangible information regarding the identity of U_x. Therefore, the step to send M_{sg3} from the SD_z to U_x is out of question. Hence, the scheme Wazid et al. is incorrect and due to this incorrectness, the said scheme fails to complete a round of authentication process.

4.3.2. Identity De-Synchronization

The provision of anonymity and user privacy in the scheme of Wazid et al. is achieved through temporary identity generated by the CS_y during registration phase and this temporary identity is updated during each login and authentication round, described as follows: The user U_x sends temporary identity TID_x as part of message M_{sg1}. The CS_y upon reception of M_{sg1} extracts RD_x corresponding to TID_x and then after processing the message generates new temporary identity TID_x^{new}, hides it in $M_T = TID_x^{new} \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_2)$ and sends it to SD_z along with other parameters included in M_{sg2}. This M_T is sent through M_{sg3} from SD_z to U_x. Finally, the U_x after processing the message updates TID_x by TID_x^{new}. Now, if any of the message M_{sg2} or M_{sg3} is blocked by an attacker controlling the public communication channel as per CK attack model adopted in this paper, the U_x would not be able to update its temporary TID_x, whereas, the CS_y has already updated TID_x by TID_x^{new}, after receiving M_{sg1}. Now, both entities U_x and CS_y are having mismatched identities. Hence, identity de-synchronization has occurred, and for the next login by U_x will fail.

CHAPTER FIVE

PROPOSED SCHEME

This section details the our proposed and improved scheme iUAKMS-NIB.

5.1. Registration Phase

This phase uses a fully Trusted Authority (TA) that selects a "nonsingular elliptic curve $E_p(a, b)$ and forms "$y2 = x3 + ax + b(modp)$ over a Galois (finite) field $GF(p)$, where p is a large prime," such that the "Elliptic Curve Discrete Logarithm Problem (ECDLP)" becomes intractable, with "a base point P in $E_p(a, b)$, whose order is as big as p.

Furthermore, the TA selects a collision-resistant one-way cryptographic hash algorithm $h(\cdot)$ along with a private key d_{TA} of the trusted authority.

Smart Industrial Device Registration

The following steps are performed by TA for registration of the deployment of a smart industrial device.

First of all, a a particular identity ID_z and a random secret key $d_z \epsilon Z_p^*$ for smart device SD_z, is chosen by the TA. For SD_z, TA calculates the pseudo identity of SD_z as $RD_z = h(ID_z \parallel d_{TA})$, the public key of d_z as $Q_z = d_z \cdot P$ and the temporal credential as $TC_z = h(d_z \parallel ID_z \parallel RTS_z \parallel d_{TA})$, where RTS_z is the registration timestamp of SD_z.

The information obtained from RSD-1, such that RD_z, TC_z, Q_z, d_z, $h(\cdot)$, $E_p(a, b)$, P is stored in the memory of SD_z before the development of SD_z. It is noted that Q_z is announced widely to the other network entities. In addition, RI d_z can be sent to CS_y by TA in a secure way.

5.2. Content Server Registration

The content server CS_y is registered during this phase. This task is executed by TA in the following steps.

The TA chooses a unique identity ID_y and a secret key $d_y = h(ID_y||d_{TA})$ for CS_y to calculate the pesudo identity of CS_y as $RD_y = h(ID_y \parallel d_{TA})$, public key $Q_y = d_y \cdot P$ & pseudo-random identity $RD_{TA} = h(ID_{TA} \parallel d_{TA})$.

The credentials RD_y, RD_x, TID_x, RD_{TA}, RD_z, Q_y, d_y, $h(\cdot)$, $E_p(a,b)$, P in CS_y is secure/tamper-resistant database by the TA.

Note that during the user registration phase, $RD_x$and $TID_x$for a registered user U_x are produced in the section below. Q_y is also made available to other network entities in the public domain.

5.3. User Registration

The TA performs the following actions to register a user U_x using a method of communication that is secure (e.g., in person) at this phase..

To generate the hidden key $RPW'_x = h(PW'_x \parallel x)$., U_x selects the user unique identify ID_x, the password RPW'_x, and a long-term random secret xZ p*. U x then uses a secure channel to communicate ID_x and $RPW'_x$to the TA.

Following receipt of the registration data,, the TA computes the pseudo identity $RD_x = h(ID_x \parallel d_{TA})$, generates temporary identity $TID_x = E_{d_{y(RD_x||r_0)}}$ (r_0 being a random number generated by TA) and a secret key $d_x = h(ID_x||d_{TA})$ for U_x. The TA computes temporal credential of U_x as $TC_x = h(ID_x \parallel RPW'_x \parallel d_x \parallel d_{TA} \parallel RTS_x)$, $\alpha'_x = h(RPW'_x \parallel RD_x) \oplus d_x$ and its public key as $Q_x = d_x \cdot P$. The TA then sends RD_x, TID_x, RD_{TA}, TC_x, α'_x, Q_x, $h(\cdot)$, $E_p(a,b)$, P to D_x of U_x through a secure channel.

It's worth noting that Q x is visible to other network entities.

Upon the reciving data from trusted autority TA, U_x furnishes biometric data BO_x access the fingerprint or other personal information stored on their mobile device. D_x to compute $(\alpha'_x, \tau_x) = Gen(BO_x)$, where α'_x and τ_x are the public reproduction parameter and the biometric secret key of l bits, respectively. and "$Gen(\cdot)/Rep(\cdot)$ are the fuzzy extractor probabilistic generation and deterministic reproduction functions, respectively (Saha et al., 2020; Wang et al., 2021)". Furthermore, U_x computes $d_x = h(RPW'_x \parallel RD_x) \oplus \alpha'_{U_x}$, $TC_x = h(TC_x \parallel x \parallel \alpha'_x)$, $x^* = x \oplus h(ID_x \parallel PW'_x\alpha'_x)$,

$RD_x^* = RD_x \oplus h(PW'_x \parallel \alpha'_x)$, $TID_x^* = TID_x \oplus h(ID_x \parallel PW'_x)$, $RD_{TA}^* = RD_{TA} \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$, $TC_x^* = TC_x \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x$, $d_x^* = d_x \oplus h(ID_x \parallel \alpha'_x)$ and $LV = h(ID_x \parallel RPW'_x \parallel TC_x \parallel d_x \parallel \alpha'_x)$. Finally, RID_x^*,TID_x^*, RD_{TA}^*, TC_x^*, d_x^*,Q_x, τ_x, LVx^*, $h(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, t, $E_p(a,b)$, P are stored in the memory of D_x. Note that α'_x, x, ID_x, RPW'_x, RD_x, TID_x, RD_{TA}, TC_x, TC_x and d_x are deleted from the memory of D_x to protect against stolen verifier, privileged insider attack, unauthorised session key computation, illegal user's password guessing and user impersonation attacks.

The TA sends the credentials RD_x, TID_x to CS_y in a secure way through a pre-shared symmetric secret key K_y, TA. The TA also erases RD_x, TID_x, RD_y, RD_z, d_x, d_y, d_z, TC_x, TC_z, α'_x, RPW'_x from its memory to protect against stolen verifier, privileged insider attack, unauthorized session key computation, illegal user's password guessing and user impersonation attacks.

5.4. User Login Phase

A valid user U_x must first log into the system in order to utilize the NIB's services. The actions below are necessary for such a proposal.U_x provides evidence of his or her identity ID_x and key PW'_x, and prints biometrics BO'_x using the accelerometer on his or her smart phone D_x in order to determine the biometric private key $\alpha'_x = Rep(BO'_x,\ \tau_x)$ provided that the "Hamming distance between the real biometrics BO_x provided during the user registration phase and current BO'_x is less than or equal to a pre-defined error tolerance threshold, say t".

U_x and calculates $\alpha'_x = Rep(BO'_x,\ \tau'_x)$, $x = x^* \oplus h(ID_x \parallel PW'_x \parallel \alpha'_x)$, $RPW'_x = h(PW'_x \parallel x)$, $RD'_x = RD_x \oplus h(PW'_x \parallel \alpha'_x)$, $TID'_x = TID_x \oplus h(ID_x \parallel PW'_x)$, $RD'_{TA} = RD_{TA} \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$, $TC'_x = TC *_x \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$, $d_x = d *_x \oplus h(ID_x \parallel \alpha'_x)$ and checks the condition $LV' \overset{?}{=} h(ID_x) \parallel RPW'_x \parallel TC'_x \parallel d_x \parallel \alpha'_x)$. If it is true, then U_x is a real user; if it is not true, then the login procedure is immediately terminated.

D_x produces a date for the current time.T_1 and a unjustified highly secret $r_x \epsilon Z_p^*$ to calculate $M_1 = h(r_x \parallel T_1) \oplus h(RD_{TA} \parallel RD_x \parallel d_x \cdot Q_y \parallel T_1)$, $MM_1 = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1)$, $M_x = h(RD_x) \parallel$

$RD_{TA})$, $M_2 = M_x \cdot P$, $M_3 = M_x + h(r_x \parallel T_1) \cdot d_x$. U_x next chooses an accessible smart phone with the pseudo identification SD_z. RD_z and sends the login message $M_{sg1} = \{TID_x, RD_z, M_1, MM_1, M_2, M_3, T_1\}$ to CS_y via open channel.

5.5. User Authentication and Key Agreement Phase

This phase is required for mutual authentication among a registered user U_x, a content server CS_y and an accessed smart industrial device SD_z. After the successful completion of the following steps, both U_x and SD_z establish a session key for their secure communication via CS_y.

After receiving M_{sg1} from U_x, CS_y first verifies the timeliness of T_1 through the condition, $|T_1 - T_1^*| \leq \Delta T$, when "maximum transmission delay" called ΔT & T_1^* is getting time at which the message was sent M_{sg1}. If the criteria are met, CS_y extracts $(RD_x || r_0) = D_{d_y}(TID_x)$. CS_y further calculates $h(r_x \parallel T_1) = M_1 \oplus h(RD_{TA} \parallel RD_x \parallel d_y \cdot Q_x \parallel T_1)$, $M_x = h(RD_x \parallel RD_{TA})$ and checks if $M_3 \cdot P = M_2 + h(r_x \parallel T_1) \cdot Q_x$. If CS_y finds this condition true, U_x is authenticated by CS_y.

CS_y compute a label with the current time T_2 and an unrelated hidden fact $r_y \epsilon Z_p^*$ to compute $M_4 = h(r_y \parallel T_2 \parallel RD_y) \oplus h(RD_z \parallel d_y \cdot Q_z \parallel T_2)$, $MM_2 = MM_1 \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$, $M_y = h(RD_z \parallel T_2)$, $M_5 = M_y \cdot P$ and the ElGamal type signature $M_6 = M_y + h(r_y \parallel T_2 \parallel RD_y) \cdot d_y$. CS_y then sends the message $M_{sg2} = \{RD_z, M_4, MM_2, M_5, M_6, T_1, T_2\}$ to SD_z through public channel.

Later receiving M_{sg2} from CS_y, SD_z Initially, he checks the timeliness. of T_2 by checking $|T_2 - T_2^*| \leq \Delta T$ where T_2^* is the message's time of receipt M_{sg2}. If it is valid, SD_z computes $h(r_y \parallel T_2 \parallel RD_y) = M_4 \oplus h(RD_z \parallel d_z \cdot Q_y \parallel T_2)$, $h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA})$, $= MM_2 \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$, $M_y = h(RD_z \parallel T_2)$ and checks $M_6 \cdot P \overset{?}{=} M_5 + h(r_y \parallel T_2 \parallel RD_y) \cdot Q_y$. If SD_z finds this condition true, CS_y is authenticated by SD_z, and SD_z sets $X_s = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA})$.

SD_z produces a timestamp for the present time. T_3 with a weird secret $r_z \epsilon Z_p^*$ calculatin $M_7 = h(r_z \parallel T_3) \oplus h(T_1 \parallel T_3 \parallel d_z \cdot Q_x)$, $M_w = h(RD_z \parallel TC_z) \oplus$

$h(h(r_z \parallel T_3) \parallel T_1)$, $M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$, $M_8 = M_z \cdot P$, session key $SK_{z,x} = h(X_s \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$, and generates the ElGamal type signature $M_9 = M_z + h(SK_{z,x} \parallel T_1 \parallel T_3) \cdot d_z$. Now, SD_z computes $M_S = h(ID_y||h(r_y \parallel T_2 \parallel RD_y||T_3)$ and then sends the message $M_S = h(ID_y||h(r_y \parallel T_2 \parallel RD_y||T_3)$ to U_x through public channel

Later obtaining M_{sg3} from SD_z, CS_y first validates the punctuality of T_3 by checking $|T_3 - T_3^*| \leq \Delta T$ where T_3^* the timing of message receipt M_{sg3}. If it is valid, CS_y further checks $M_S \overset{?}{=} h(ID_y||h(r_y \parallel T_2 \parallel RD_y||T_3)$ and on verification it computes new pseduo and temporary identity $TID_x^{new} = E_{d_y}(RD_x||r_y)$ for U_x and then generates current T_4 to compute $M_T = TID_x^{new} \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_4)$, $M_C = h(TID_x^{new}||T_4||TID_x)$ and sends $M_{sg4} = \{M_{sg3}, M_T, M_C, T_3, T_4\}$ to U_x.

After receiving M_{sg4} from CS_y and after successful verification of the timeliness of T_4, U_x computes $h(r_z \parallel T_3) = M_7 \oplus h(T_1 \parallel T_3 \parallel Q_z \cdot d_x)$, $h(RD_z \parallel TC_z) = M_w \oplus h(h(r_z \parallel T_3) \parallel T_1)$, $M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$, and session key $SK_{x,z} = h(h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$, and checks $M_9 \cdot P \overset{?}{=} M_8 + h(SK_{x,z} \parallel M_T \parallel T_1 \parallel T_3) \cdot Q_z$. SD_z is authentic if this condition holds; else, U_x instantly aborts the procedure. U_x also computes $TID_x^{new} = M_T \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_4)$ and checks $M_C \overset{?}{=} h(TID_x^{new}||T_4||TID_x)$ In addition and if the above condition is true U_x replaces TID_x with TID_x^{new} in Its recollection data will be used in future sessions.

Table 3. Proposed Scheme

User ($\boldsymbol{U_x}$) / Mobile Device ($\boldsymbol{D_x}$)	Content Server ($\boldsymbol{CS_y}$)	Smart Industrial Device ($\boldsymbol{SD_z}$)
Submit ID_x, PW'_x, BO'_x Computes $\alpha'_x = Rep(BO'_x, \tau'_x)$		

$x = x^* \oplus h(ID_x \parallel PW'_x \parallel \alpha'_x)$ $RPW'_x = h(PW'_x \parallel x)$ $RD'_x = RD_x \oplus h(PW'_x \parallel \alpha'_x)$, $TID'_x = TID_x \oplus h(ID_x \parallel PW'_x)$ $RD'_{TA} = RD_{TA} \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$ $TC'_x = TC *_x \oplus h(ID_x \parallel RPW'_x \parallel \alpha'_x)$ $d_x = d *_x \oplus h(ID_x \parallel \alpha'_x)$ Check $LV' \overset{?}{=} h(ID_x) \parallel RPW'_x \parallel TC'_x \parallel d_x \parallel \alpha'_x)$ Generate T_1, $r_x \epsilon Z_p^*$ & Compute $M_1 = h(r_x \parallel T_1) \oplus h(RD_{TA} \parallel RD_x \parallel d_x \cdot Q_y \parallel T_1)$		

$MM_1 = h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_1)$ $M_x = h(RD_x) \parallel RD_{TA})$ $M_2 = M_x \cdot P$ $M_3 = M_x + h(r_x \parallel T_1) \cdot d_x$ $M_{sg1}=\{TID_x,RD_z,M_1,MM_1,M_2,M_3$		
	Verifies T_1 Extract $\boxed{(RD_x \mid\mid r_0) = D_{d_y}(TID_x)}$ and compute $h(r_x \parallel T_1) = M_1 \oplus h(RD_{TA} \parallel RD_x \parallel d_y \cdot Q_x \parallel T_1)$ $M_x = h(RD_x \parallel RD_{TA})$ Check $M_3 \cdot P = M_2 + h(r_x \parallel T_1) \cdot Q_x$ Generate T_2, $r_y \epsilon Z_p^*$ & Compute	

	$M_4 = h(r_y \parallel T_2$ $\parallel RD_y) \oplus h(RD_z$ $\parallel d_y \cdot Q_z \parallel T_2)$ MM_2 $= MM_1 \oplus h(h(r_x$ $\parallel T_1) \parallel RD_{TA}$ $\parallel T_1) \oplus h(h(r_y \parallel T_2$ $\parallel RD_y) \parallel T_2 \parallel RD_z)$ $M_y = h(RD_z \parallel T_2)$ $M_5 = M_y \cdot P$ $M_6 = M_y +$ $h(r_y \parallel T_2 \parallel RD_y) \cdot d_y$ M_{sg2}={RD_z,M_4,MM_2,M_5,M_6,T_1,	
		Verify T_2 and Compute $h(r_y \parallel T_2 \parallel RD_y) =$ $M_4 \oplus h(RD_z \parallel d_z \cdot Q_y \parallel T_2)$ $h(h(r_x \parallel T_1) \parallel TC_x \parallel$ $T_1 \parallel RD_x \parallel RD_{TA})$ $= MM_2 \oplus h(h(r_x \parallel$ $T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_x \parallel$ $T_1) \parallel RD_{TA} \parallel T_1) \oplus h(h(r_y \parallel$ $T_2 \parallel RD_y) \parallel T_2 \parallel RD_z)$ $M_y = h(RD_z \parallel T_2)$ $M_6 \cdot P \overset{?}{=} M_5 + h(r_y \parallel$ $T_2 \parallel RD_y) \cdot Q_y$ $X_s = h(h(r_x \parallel T_1) \parallel$ $TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA})$ Generate $T_3, r_z \epsilon Z_p^*$ & Compute $M_7 = h(r_z \parallel T_3) \oplus$ $h(T_1 \parallel T_3 \parallel d_z \cdot Q_x)$ $M_w = h(RD_z \parallel$ $TC_z) \oplus h(h(r_z \parallel T_3) \parallel T_1)$ $M_z = h(h(RD_z \parallel TC_z) \parallel T_1$ $\parallel T_3)$ $M_8 = M_z \cdot P$

		$SK_{z,x} = h(X_s \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$ $M_9 = M_z + h(SK_{z,x} \parallel T_1 \parallel T_3) \cdot d_z$ $\boxed{M_S = h(ID_y \Vert h(r_y \parallel T_2 \parallel RD_y \vert}$ $\xleftarrow{M_{sg3}=\{M_7,M_w,M_8,M_9,\boxed{M_S},T_3\}}$
	$M_S \overset{?}{=} h(ID_y \Vert h(r_y \parallel T_2 \parallel RD_y \Vert T_3)$ $TID_x^{new} = E_{d_y}(RD_x \Vert r_y)$ Generate T_4 $M_T = TID_x^{new} \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_4)$ $M_C = h(TID_x^{new} \Vert T_4 \Vert TID_x)$ $\xleftarrow{M_{sg4}=\{M_{sg3},M_T,M_C,T_3,T_4\}}$	
Verifies T_3 & $\boxed{T_4}$ and Compute $h(r_z \parallel T_3) = M_7 \oplus h(T_1 \parallel T_3 \parallel Q_z \cdot d_x)$ $h(RD_z \parallel TC_z) = M_w \oplus h(h(r_z \parallel T_3) \parallel T_1)$		

$M_z = h(h(RD_z \parallel TC_z) \parallel T_1 \parallel T_3)$ $SK_{x,z} = h(h(h(r_x \parallel T_1) \parallel TC_x \parallel T_1 \parallel RD_x \parallel RD_{TA}) \parallel h(r_z \parallel T_3) \parallel T_1 \parallel T_2 \parallel T_3 \parallel M_z)$ Check $M_9 \cdot P \overset{?}{=} M_8 + h(SK_{x,z} \parallel M_T \parallel T_1 \parallel T_3) \cdot Q_z$ $TID_x^{new} = M_T \oplus h(h(r_x \parallel T_1) \parallel RD_{TA} \parallel T_4)$ $M_C \overset{?}{=} h(TID_x^{new} \Vert T_4 \Vert TID_x$ Replace TID_x with TID_x^{new}		

CHAPTER SIX

PERFORMANCE ANALYSİS

This section evaluates the performance of the proposed scheme in terms of computation cost, and communication cost of the proposed scheme with the existing schemes. The details are given in the following subsections.

6.1. Computational Cost Analysis

The subsection presents a high-level overview of the comparative computing cost study of our method and similar schemes such as (Antwi-Boasiako et al., 2021; Bowman et al., 2002; Bäck & Schwefel, 1993; Freitas, 2003; Nesmachnow, 2014; Paulin & Knight, 1989). A real-time environment is set up and an experiment is done by using the MIRACL Library on a smartphone, the iPhone Xs Max, which has 8 GB of RAM and a Dual Core + 1.6 GHz Quad-Core Processor. The underlying IOS operating system version is version 15.1. In other words, the iPhone Xs Max is used and represents a user/mobile device in this experiment. The Dell Ultrabook 8757P, with an Intel Core i5-6300C processor and 8 GB of RAM, was used as a content server, with the Windows 10 Pro operating system running on top of the machine. In a similar way, a Raspberry Pi 3 B+ with a Cortex-A53 (ARMv8) 64-bit SoC running at 1.4 GHz and 1 GB of LPDDR2 SDRAM RAM are used to simulate a smart device. Table 4 contains the simulation results for each device; also, following the analogy of (Ali et al., 2021), it is considerd that $T_f \approx T_e$, where T_f is the running time of executing a fuzzy extractor and T_e is the time used to compute the results. According to the experimental results, the proposed scheme may complete the authenticated process in about 59.00 milliseconds at a cost of $40\ T_h + 16T_e + 3T_a + 3T_r$. In comparison to the schemes such as (Wazid et al., 2020), (Hussain et al., 2021), (Jia et al., 2019), (Chang & Le, 2015), and (Challa et al., 2020), complete the authentication processes in about 60.428, 32.929, 58.561, 14.339, and 12.574 milliseconds, respectively. According to the computational cost, the Challa et al. performs the best; however, the proposed scheme is significantly more secure than the rest of the schemes.The comparison is each of the entity is given in the Table 5.

Table 4: Experimental Results

↓Operation/ Device→	Mobile	Server	Drone
T_b: Bi-linear Pairing	17.36	4.038	12.52
T_e: Point Multiplication	5.116	0.926	4.107
T_a: Point Addition	0.013	0.006	0.018
T_h: One way Hash	0.009	0.004	0.006
T_r: Random Number Generation	2.011	0.118	1.185
T_{se}: Symmetric Key Operations	0.017	0.08	0.013

Table 5: Computational Costs

Reference	*Mobile User*	*Content Server*	*Smart Device*	*RT(ms)*
Proposed	$19T_h + 6T_e + T_a + T_r$	$11T_h + 6T_e + T_a + T_r$	$12T_h + 5T_e + T_a + T_r$	60.425
Wazid et al.	$8T_h + 2T_e + 2T_r$	$7T_h + T_e$	$6T_h + 4T_e + T_r$	32.929
Hussain et al.	$5T_h + 2T_e + T_r + T_b$	$9T_h + 3T_e + T_r + T_b$	$4T_h + 2T_e + T_r + T_b$	58.561
Jia et al.	$6T_h + 2T_e + T_r$	$6T_h + 2T_e + T_r$	$8T_h$	14.339
Chang et al.	$11T_h + T_e + T_r$	$5T_h$	$6T_h + T_e + T_r$	12.574
Challa et al.	$19T_h + 6T_e + T_a + T_r$	$9T_h + 5T_e + T_a + 2T_{sc} + T_r$	$12T_h + 5T_e + T_a + T_r$	59.651

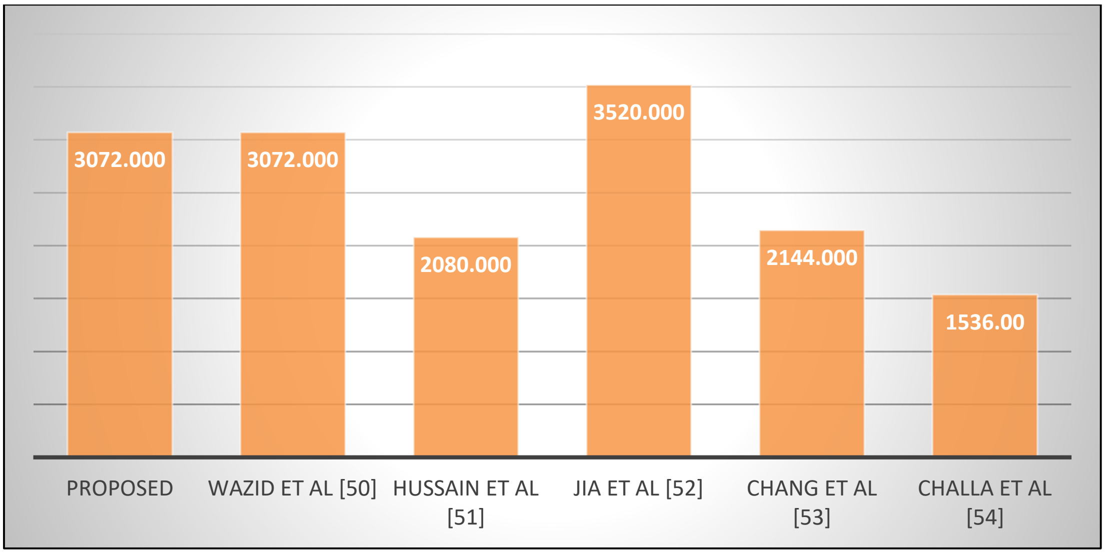

Figure 6: Graphical Representation of Computational Cost

6.2. Communication Cost

In this section, the communication cost of the proposed scheme is calculated and compared with the existing schemes. Table 6 displays a size of different metric entities used in the proposed scheme. For the sake of comparison and simplicity, the size of user identities is taken to be 64 bits long, the timestamp is 32 bits, the hash function is 160 bits, the random number is 64 bits, encryption (AES) is 128 bits, and the size of the Eliptic Curve (ECC) is fixed at 320 bits in order to maintain a comparable security level with 1024 bits RSA. Table 7 displays a detailed comparison among the suggested schemes presented with regard to the bits transferred. The cost of communication of the proposed scheme is 3072 bits, which is equal to Wazid's et al. scheme. The total communication cost of Jia et al. is 3520 bits, which is slightly higher than the proposed scheme. In contrast, the overall communication expenses of Challa et al., Hussain et al., and Chang et al., are 1536 bits, 2080 bits, and 2144 bits, respectively; which are less than the proposed scheme. However, the proposed scheme provides a better authentication scheme than all the above mentioned schemes.

Table 6: Communication Cost Values

Attribute	**Cost Value**
Identity	64 bits
Timestamp	32 btis
Hash Function (SHA-1)	160 btis
Random Number	64 btis
Encryption (AES)	128 btis
Elliptic Curve (ECC)	320 btis

Table 7: Communication Cost Analysis

Reference	**User (U_x)**	**Content Server (CS_y)**	**Smart Device (SD_z)**	**Total Cost**
Proposed	800 bits	928 + 352 bits	992 bits	3072 bits
Wazid et al.	1056 bits	1088 bits	928 bits	3072 bits
Hussain et al.	896 bits	672 bits	512 bits	2080 bits
Jia et al.	672 bits	1344 + 832 bits	672 bits	3520 bits
Chang et al.	672 bits	608 + 352 bits	512 bits	2144 bits
Challa et al.	672 bits	352 bits	512 bits	1536 bits

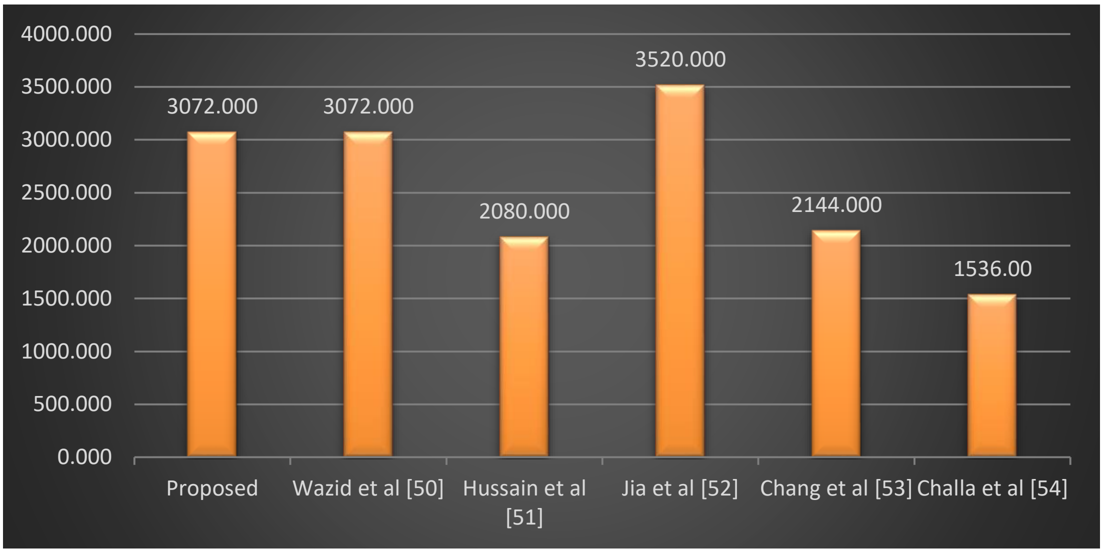

Figure 7: Graphical Representation of Communication Cost

8 The Security Analysis

To describe the security of the proposed scheme, we have scrutinized the scheme through formal and informal security analysis in the following subsections:

6.3. Authentication proof based on the Burrows–Abadi–Needham Logic (BAN Logic)

The security of the proposed scheme is formally analyzed in the standard model using the widely accepted Burrows–Abadi– Needham logic.

6.3.1. Postulates for BAN Logic

Some of the logical postulates of BAN logic and the meaning related to the postulates are given below in Table 8:

Table 8: Postulates for BAN logic

$\frac{A\| \equiv A \overset{K}{\leftrightarrow} Y, A \lhd < B >_K}{A\| \equiv Y\| \sim K}$	Message-meaning rule
$\frac{A\| \equiv \#B, A\| \equiv Y\| \sim B}{A\| \equiv Y\| \sim K}$	Nonce-verification rule
$\frac{A\| \equiv B, A\| \equiv C}{A\| \equiv (B, C)}$	Belief Rule

$\frac{A\| \equiv \#B, A\| \equiv C}{A\| \equiv \#(B, C)}$	Fresh conjuncatenation rule
$\frac{A\| \equiv Y \Rightarrow B, A\| \equiv Y\| \sim B}{A\| \equiv B}$	Jurisdiction rule

6.3.2. Security Goal Establishment

Established security goals and logical notations of the BAN logic are given below in Table 9.

$$G_1: U_x| \equiv SD| \equiv Ux \overset{SK_{x,y}}{\longleftrightarrow} SD$$

Table 9: BAN Logic Notations

$\boldsymbol{A\| \equiv B}$	A believes a statement B
$\boldsymbol{A \overset{K}{\longleftrightarrow} Y}$	Share a key K between A and Y
$\#\boldsymbol{B}$	B is fresh
$\boldsymbol{A \lhd B}$	A sees B
$\boldsymbol{A\| \sim B}$	A said B
$(\boldsymbol{B, C})_{\boldsymbol{K}}$	B, C is hashed by key K
$\{\boldsymbol{B}\}_{\boldsymbol{K}}$	B is hashed with key K
$< \boldsymbol{B} >_{\boldsymbol{K}}$	B is encrypted with key K

6.3.3. Proposed Schemes Idealized Form using BAN Logic

M1: $SD \rightarrow U_x : (h(r_z||T_3) \oplus h(T_1||T_2||T_3||d_z||Q_x)), h(RD_z||TC_z) \oplus h(h(r_z||T_3)||T_1), Mz.P, Mz\ (SKz, x||T_1||T_3).dz, h(ID_y||h(r_y||T_z||RDy||T_3), T_3), TID_x^{new} \oplus h(h(r_x, T_1)||RD_{TA}||T_4), h(TID_x^{new}||T_4||TID_x), (T_3, t4)$

6.3.4. Assumptions

1. $A1: U_x| \equiv \grave{}\#(r_x, T1)$
2. $A2: U_x| \equiv SD| \equiv SD \sim X$
3. $A3: U_x| \equiv SD \Rightarrow (SD \overset{SK_l x}{\leftrightarrow} SD)$
4. $A4: SD| \equiv CS \Rightarrow CS| \sim X$
5. $A5: CS| \equiv (r_y, T_4, T_2)$
6. $A6: SD| \equiv \#(r_z, T_3)$
7. $A7: U_x| \equiv (U_x \overset{RD_x}{\leftrightarrow} CS)$
8. $A8: SD| \equiv (CS \overset{RD_z}{\leftrightarrow} SD)$
9. $A9: SD| \equiv (CS \overset{dz}{\leftrightarrow} SD)$
10. $A10: U_x| \equiv (U_x \overset{RD_{TA}}{\leftrightarrow} CS)$
11. $A11: U_x| \equiv (U_x \overset{TID_x}{\leftrightarrow} CS)$
12. $A12: U_x| \equiv (U_x \overset{TID_x}{\leftrightarrow} SD)$
13. $A13: U_x| \equiv CS| \Rightarrow CS| \sim X$
14. $A14: SD| \equiv (SD \overset{RD_{TA}}{\leftrightarrow} M_z)$

Step 1: According to Message 1:

$$P1: U_x\ U_x \overset{Q_x}{\leftrightarrow} SD, T_1, T_3, d_z\rangle_{\langle rz\rangle}, \langle U_x \overset{RD_z}{\leftrightarrow} SD, TC_z, T_1, T_3\rangle_{\langle rz\rangle}, \langle M_z.P\rangle, \langle M_z, T_1, T_3\rangle_{\langle U_x \overset{SK_{zx}}{\leftrightarrow} SD, d_z\rangle},$$

$$\langle ID_y, U_x \overset{RD_y}{\leftrightarrow} SD, T_2, T_3\rangle_{\langle}ry\rangle, \langle T_3\rangle, \langle U_x \overset{RD_x}{\leftrightarrow} CS, TID_x, T_1, T_4\rangle\ U_x \overset{r_x}{\leftrightarrow} SD,$$

$$\langle U_x \overset{TID_x}{\leftrightarrow} CS, T_3, T_4\rangle_{\langle TID_x^{new}\rangle}$$

Step 2: Based on P1, Assumptions 1,2,3 and message meaning rule we get:

- $P2: U_x \lhd$ $\langle T_1, T_2, d_z\rangle_{\langle rz\rangle}, \langle T_1, T_3, TC_z\rangle_{\langle rz\rangle}, \langle Mz.P\rangle, \langle M_z, T_2, T_3\rangle_{\langle dz\rangle}, \langle ID_y, T_1, T_3\rangle_{\langle ry\rangle}, \langle T_3\rangle, \langle T_1, T_4\rangle_{\langle TID_x^{new}}$

Step 3: According to the P2 and message belief rule, nonce verification and freshness rule we get:

- $P3: U_x| \equiv CS| \equiv \langle dz\rangle_{\langle rz\rangle}, \langle TC_z\rangle_{\langle rz\rangle}, \langle Mz.P\rangle, \langle Mz\rangle_{\langle dz\rangle}, \langle ID_y\rangle_{\langle ry\rangle}$

Step 4: Based on S3, Assumptions A2 and A13 and jurisdiction rule are obtained:

- $P4: U_x| \equiv \langle dz\rangle_{\langle rz\rangle}, \langle TCz\rangle_{\langle rz\rangle}, \langle Mz.P\rangle, \langle Mz\rangle_{\langle dz\rangle}, \langle ID_y\rangle_{\langle ry\rangle}$

Step 5: Based on P4 and P3 and assumptions A2, A13, A14 and belief rule are used to obtained the value:

- $P5: U_x| \equiv SD| \equiv Ux \overset{SK_{x,y}}{\leftrightarrow} SD$

CONCLUSION

In this thesis, the Wazid el al. scheme is analyzed and found some incorrectness. An authentication scheme is proposed in Wazid et al. for the NIB-enabled 6G networking systems. On the other hand, a critical step in the plan was overlooked at the content server, resulting in a complete failure of the whole scheme. As a consequence, the approach is deemed ineffective, and the authentication activity is unable to be performed as planned. According to the research's authors, a modified version of the technique has been developed in order to give a more dependable authentication process. There is a thorough comparison of the suggested approach with current systems in terms of computation costs and communication expenses included in the study. In addition, the security analysis is included into this plan of action for maximum effectiveness.

In order to tackle these flaws, this work suggested an updated approach based on elliptic curve, which enables user authentication and greater security.

The important contributions of this thesis are as follows:

- An enhanced remote user authentication approach The iUAKMS-NIB is an encrypted communication protocol for use in 6G-enabled NIBs that are used for commercial applications and is available for download. Once a smart industrial device has been authenticated using the iUAKMS-NIB, a verified user may access the device's real-time data using the establish session key that was generated when the device was authenticated.
- This thesis presented the security analysis, as well as the formal security verification by utilizing the widely acknowledged program ProVerif, a tool used for automatically studying the security of cryptographic protocols. It is proved that the iUAKMS-NIB is robust against a range of conceivable threats that are required in an NIB environment to support 6G.
- Finally, a detailed comparison investigation between the updated iUAKMS-NIB and UAKMS-NIB rival login systems demonstrates

that the achievement of iUAKMS-NIB is superior to the performance of other current competing schemes in terms of user authentication.

In the not-too-distant future, the authors predict, this technology will be implemented in the Internet of Things-based networking system that they have developed.

REFERENCES

Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security Requirements and Challenges of 6G Technologies and Applications. *Sensors*, *22*(5), 1969.

Akyildiz, I. F., Jornet, J. M., & Han, C. (2014). Terahertz band: Next frontier for wireless communications. *Physical communication*, *12*, 16-32.

Ali, Z., Chaudhry, S. A., Mahmood, K., Garg, S., Lv, Z., & Zikria, Y. B. (2021). A clogging resistant secure authentication scheme for fog computing services. *Computer Networks*, *185*, 107731.

Antwi-Boasiako, E., Zhou, S., Liao, Y., Liu, Q., Wang, Y., & Owusu-Agyemang, K. (2021). Privacy preservation in Distributed Deep Learning: A survey on Distributed Deep Learning, privacy preservation techniques used and interesting research directions. *Journal of Information Security and Applications*, *61*, 102949.

Avispa, T. (2015). Automated validation of internet security protocols and applications. In.

Basar, E. (2019). Transmission through large intelligent surfaces: A new frontier in wireless communications. 2019 European Conference on Networks and Communications (EuCNC),

Bowman, D. A., Gabbard, J. L., & Hix, D. (2002). A survey of usability evaluation in virtual environments: classification and comparison of methods. *Presence: Teleoperators & Virtual Environments*, *11*(4), 404-424.

Bäck, T., & Schwefel, H.-P. (1993). An overview of evolutionary algorithms for parameter optimization. *Evolutionary computation*, *1*(1), 1-23.

Canetti, R., & Krawczyk, H. (2001). Analysis of key-exchange protocols and their use for building secure channels. International conference on the theory and applications of cryptographic techniques,

Challa, S., Das, A. K., Gope, P., Kumar, N., Wu, F., & Vasilakos, A. V. (2020). Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. *Future Generation Computer Systems*, *108*, 1267-1286.

Chang, C.-C., & Le, H.-D. (2015). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on wireless communications*, *15*(1), 357-366.

Chen, S., Liang, Y.-C., Sun, S., Kang, S., Cheng, W., & Peng, M. (2020). Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed. *IEEE Wireless Communications*, *27*(2), 218-228.

Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open Journal of the Communications Society*, *1*, 957-975.

Freitas, A. A. (2003). A survey of evolutionary algorithms for data mining and knowledge discovery. In *Advances in evolutionary computing* (pp. 819-845). Springer.

Gui, G., Liu, M., Tang, F., Kato, N., & Adachi, F. (2020). 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wireless Communications*, *27*(5), 126-132.

Hussain, S., Chaudhry, S. A., Alomari, O. A., Alsharif, M. H., Khan, M. K., & Kumar, N. (2021). Amassing the security: An ECC-based authentication scheme for Internet of drones. *IEEE Systems Journal*, *15*(3), 4431-4438.

Jia, X., He, D., Kumar, N., & Choo, K.-K. R. (2019). Authenticated key agreement scheme for fog-driven IoT healthcare system. *Wireless Networks*, *25*(8), 4737-4750.

Mookherji, S., Odelu, V., & Prasath, R. (2022). Analysis of A Lightweight Authentication Protocol for Remote Surgery Applications under the CK-Adversary Model. 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS),

Nesmachnow, S. (2014). An overview of metaheuristics: accurate and efficient methods for optimisation. *International Journal of Metaheuristics*, *3*(4), 320-347.

Padhi, P. K., & Charrua-Santos, F. (2021). 6G enabled industrial internet of everything: towards a theoretical framework. *Applied System Innovation*, *4*(1), 11.

Paulin, P. G., & Knight, J. P. (1989). Force-directed scheduling for the behavioral synthesis of ASICs. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *8*(6), 661-679.

Pozza, M., Rao, A., Flinck, H., & Tarkoma, S. (2018). Network-in-a-box: A survey about on-demand flexible networks. *IEEE Communications Surveys & Tutorials*, *20*(3), 2407-2428.

Ram, S. B., & Odelu, V. (2022). Security Analysis of a Key Exchange Protocol under Dolev-Yao Threat Model Using Tamarin Prover. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC),

Ramaswamy, V., & Correia, J. T. (2018). Enhancing service availability of LTE-in-a-box systems using 3GPP-compliant strategies. MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), Saha, S., Sutrala, A. K., Das, A. K., Kumar, N., & Rodrigues, J. J. (2020). On the design of blockchain-based access control protocol for IoT-enabled healthcare applications. ICC 2020-2020 IEEE International Conference on Communications (ICC),

Samdanis, K., & Taleb, T. (2020). The road beyond 5G: A vision and insight of the key technologies. *IEEE Network, 34*(2), 135-141.

Sarieddeen, H., Alouini, M.-S., & Al-Naffouri, T. Y. (2019). Terahertz-band ultra-massive spatial modulation MIMO. *IEEE Journal on Selected Areas in Communications*, *37*(9), 2040-2052.

Sizer, T., Samardzija, D., Viswanathan, H., Le, S. T., Bidcar, S., Dom, P., . . . Pfeiffer, T. (2021). Integrated solutions for deployment of 6G mobile networks. *Journal of Lightwave Technology*.

Strinati, E. C., Barbarossa, S., Gonzalez-Jimenez, J. L., Ktenas, D., Cassiau, N., Maret, L., & Dehos, C. (2019). 6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication. *IEEE Vehicular Technology Magazine*, *14*(3), 42-50.

Sun, Y., Liu, J., Wang, J., Cao, Y., & Kato, N. (2020). When machine learning meets privacy in 6G: A survey. *IEEE Communications Surveys & Tutorials*, *22*(4), 2694-2724.

Thyagaturu, A. S., Dashti, Y., & Reisslein, M. (2016). SDN-based smart gateways (Sm-GWs) for multi-operator small cell network management. *IEEE Transactions on Network and Service Management*, *13*(4), 740-753.

Viswanathan, H., & Mogensen, P. E. (2020). Communications in the 6G era. *IEEE Access*, *8*, 57063-57074.

Wang, C.-X., Di Renzo, M., Stanczak, S., Wang, S., & Larsson, E. G. (2020). Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges. *IEEE Wireless Communications*, *27*(1), 16-23.

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. *Digital Communications and Networks*, *6*(3), 281-291.

Wang, W., Qiu, C., Yin, Z., Srivastava, G., Gadekallu, T. R., Alsolami, F., & Su, C. (2021). Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet of Things Journal*.

Wazid, M., Das, A. K., Kumar, N., & Alazab, M. (2020). Designing authenticated key management scheme in 6G-enabled network in a box deployed for industrial applications. *IEEE Transactions on Industrial Informatics*, *17*(10), 7174-7184.

Wikström, G., Peisa, J., Rugeland, P., Johansson, N., Parkvall, S., Girnyk, M., . . . Da Silva, I. L. (2020). Challenges and technologies for 6G. 2020 2nd 6G wireless summit (6G SUMMIT), Yang, H., Alphones, A., Xiong, Z., Niyato, D., Zhao, J., & Wu, K. (2020). Artificial-intelligence-enabled intelligent 6G networks. *IEEE Network, 34*(6), 272-280.

Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., . . . Liyanage, M. (2020). 6g white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*.

Zhang, S., & Zhu, D. (2020). Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. *Computer Networks*, *183*, 107556.

RESUME

Personal Information

Surname, name	: IJAZ UL HAQ DARMAN
Nationality	: AFGHAN

Education

Degree	Education Unit	Graduation Date
Master	Electrical and Electronics Engineering	8/8/2022
Bachelor	Computer Systems Engineering	19/11/2018
High School	Pre-engineering	04/6/2014

Work Experience

Year	Place	Title
2018	kabul	High Peace Counsel

Foreing Language

1: Englsih 2: Persian 3: Urdu

Publications

Designing an Enhanced User Authenticated Key Management Scheme for 6G-based Industrial Applications IEE Access

Hobbies

Football, Cricket, Hiking