DATA ENCRYPTION IN 6G NETWORKS: A ZERO KNOWLEDGE PROOF MODEL

A PROJECT REPORT

Submitted by

SAMYUKTA KURIKALA [RA2011003010342]

TANMAY SHARMA [RA2011003010349]

Under the Guidance of

DR.SELVARAJ.P

Associate Professor, Department of Computing Technologies

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING

DEPARTMENT OF COMPUTING TECHNOLOGIES

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR- 603 203

MAY 2024

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR–603 203

BONAFIDE CERTIFICATE

Certified that 18CSP109L project report titled "**Data Encryption in 6G Networks:A Zero Knowledge Proof Model**" is the bonafide work of **SAMYUKTA KURIKALA [RA2011003010342]** and **TANMAY SHARMA [RA2011003010349]** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported here does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate.

SUPERVISOR
Dr.P.SELVARAJ
Associate Professor
Department of Computing Technologies

PANEL HEAD
Dr.P.SELVARAJ
Associate Professor
Department of Computing Technologies

HEAD OF THE DEPARTMENT
Dr. M. PUSHPALATHA
Professor and Head
Department of Computing Technologies

INTERNAL EXAMINER

EXTERNAL EXAMINER

Department of Computational Intelligence
SRM Institute of Science & Technology
Own Work* Declaration Form

This sheet must be filled in (each box ticked to show that the condition has been met). It must be signed and dated along with your student registration number and included with all assignments you submit – work will not be marked unless this is done.

To be completed by the student for all assessments

Degree/ Course **:** B.Tech in Computer Science and Engineering

Student Name **:** SAMYUKTA KURIKALA, TANMAY SHARMA

Registration Number **:** RA2011003010342, RA2011003010349

Title of Work : Data Encryption in 6G Networks:A Zero Knowledge Proof Model

I / We hereby certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism**, as listed in the University Website, Regulations, and the Education Committee guidelines.

I / We confirm that all the work contained in this assessment is my / our own except where indicated, and that I / We have met the following conditions:

- Clearly referenced / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web, etc)
- Given the sources of all pictures, data etc. that are not my own
- Not made any use of the report(s) or essay(s) of any other student(s) either past or present
- Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
- Compiled with any other plagiarism criteria specified in the Course handbook / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

DECLARATION:
I am aware of and understand the University's policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above. **Student 1 Signature:** **Student 2 Signature:** **Date:**
If you are working in a group, please write your registration numbers and sign with the date for every student in your group.

ACKNOWLEDGEMENT

We express our humble gratitude to **Dr. C. Muthamizhchelvan**, Vice-Chancellor, SRM Institute of Science and Technology, for the facilities extended for the project work and his continued support.

We extend our sincere thanks to **Dr. T. V. Gopal** Dean-CET, SRM Institute of Science and Technology, for his invaluable support.

We wish to thank **Dr. Revathi Venkataraman**, Professor and Chairperson, School of Computing, SRM Institute of Science and Technology, for her support throughout the project work.

We are incredibly grateful to our Head of the Department, **Dr. M. Pushpalatha,** Professor, Department of Computing Technologies, SRM Institute of Science and Technology, for her suggestions and encouragement at all the stages of the project work.

We want to convey our thanks to our Project Coordinators, **Dr. S. Godfrey Winster**, Associate Professor, **Dr. M. Baskar**, Associate Professor, **Dr. P. Murali**, Associate Professor, **Dr. J. Selvin Paul Peter**, Associate Professor, **Dr. C. Pretty Diana Cyril**, Assistant Professor and **Dr. G. Padmapriya**, Assistant Professor, Panel Head, **Dr. P. Selvaraj**, Associate Professor and Panel Members, **Dr. K. Geetha**, Assistant Professor, **Dr. V. Bibin Christopher**, Assistant Professor, **Dr. M. Suresh Anand**, Assistant Professor and **Dr. P. Rama**, Assistant Professor, Department of Computing Technologies, SRM Institute of Science and Technology, for their inputs during the project reviews and support.

We register our immeasurable thanks to our Faculty Advisor, **Dr. A. Anbarasi**, Assistant Professor, Department of Computing Technologies, SRM Institute of Science and Technology, for leading and helping us to complete our course.

Our inexpressible respect and thanks to our guide, **Dr. P. Selvaraj**, Associate Professor, Department of Computing Technologies, SRM Institute of Science and Technology, for providing us with an opportunity to pursue our project under his mentorship. He provided us with the freedom and support to explore the research topics of our interest. His passion for solving problems and making a difference in the world has always been inspiring.

We sincerely thank all the staff and students of the Computing Technologies Department, School of Computing, S.R.M Institute of Science and Technology, for their help during our project. Finally, we would like to thank our parents, family members, and friends for their unconditional love, constant support and encouragement.

SAMYUKTA KURIKALA [RA2011003010342]

TANMAY SHARMA [RA2011003010349]

ABSTRACT

This work introduces a novel algorithm designed to address the pressing security challenges anticipated in 6G networks. Leveraging a combination of AES, RSA, and zero-knowledge proofs, the algorithm offers a robust framework for enhancing data security and privacy within the context of advanced wireless communication systems. AES and RSA, renowned for their encryption capabilities, are seamlessly integrated to facilitate secure data transmission and key exchange processes in 6G networks. Furthermore, the incorporation of zero-knowledge proofs adds an additional layer of security, allowing entities to validate their knowledge without compromising sensitive information.Through extensive simulations and analyses, the efficacy of the proposed algorithm in ensuring secure communication within 6G networks is demonstrated. By showcasing the algorithm's ability to mitigate potential security threats and vulnerabilities, this research lays the groundwork for the development of resilient and trustworthy next-generation communication infrastructures. Overall, the integration of AES, RSA, and zero-knowledge proofs presents a promising approach to fortifying data security in 6G networks, paving the way for safer and more reliable wireless communication technologies in the future.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AES	Advanced Encryption Standard
RSA	Rivest, Shamir, Adleman.
ZKP	Zero Knowledge Proof
zk-STARK	Zero-Knowledge Scalable Transparent Argument of Knowledge
ECB	Electronic Code Book
CBC	Cipher Block Chaining
GCM	Galois/Counter Mode
UE	User Equipment
IoT	Internet of Things
AKA	Authentication and Key Arrangement
ECDH	Elliptic-curve Diffie–Hellman
SHA-256	Secure Hash Algorithm 256
TLS	Transport Layer Security

CHAPTER 1

INTRODUCTION

1.1 The Evolution of 6G

As the world moves towards the era of 6G networks, there is a growing anticipation of revolutionary advancements in wireless communication technologies. Building upon the foundation laid by its predecessor, 5G, 6G networks are poised to redefine connectivity, communication, and the way we interact with the digital world. Unlike incremental improvements seen in previous generational shifts, the transition to 6G represents a leap forward in terms of capabilities, bringing a new era of very low data rates, latency, and ubiquitous connectivity.

At the core of the 6G vision is the promise of ultra-fast data rates that surpass those achievable with 5G networks. While 5G networks already deliver multi-gigabit-per-second speeds, 6G is expected to push the boundaries further, with data rates potentially exceeding 1 terabit per second (Tbps). Such blistering speeds hold the potential to transform various industries, enabling real-time immersive experiences, high-definition streaming, and instant data transfer on an unprecedented scale.

Moreover, 6G networks are projected to offer ultra-low latency, possibly reaching below 0.1 milliseconds (ms). This near-instantaneous response time opens the door to applications requiring instantaneous communication, such as remote surgery, autonomous vehicles, and augmented reality experiences. By minimizing latency to imperceptible levels, 6G networks aim to blur the line between physical and virtual environments, ushering in a new era of seamless connectivity.

Another key focus of 6G development is the enhancement of spectral efficiency and network coverage. By optimizing spectrum utilization and deploying advanced antenna technologies, 6G networks seek to deliver enhanced coverage, even in remote and challenging environments. This ubiquitous connectivity is essential for enabling ubiquitous connectivity, supporting applications like, from smart cities and autonomous systems to rural connectivity initiatives.

Furthermore, 6G networks are designed to accommodate the exponential growth of connected devices and the proliferation of IoT applications. With a focus on supporting massive machine-type communication, 6G networks aim to facilitate seamless connectivity for billions of devices. This capability is crucial for unlocking the full potential of emerging technologies such as smart infrastructure, intelligent transportation systems, and industrial automation.

However, alongside the promises of 6G come challenges, particularly in the realm of security. As connectivity becomes more pervasive and data volumes soar, ensuring robust security measures becomes paramount. 6G networks must address emerging threats such as quantum computing attacks, sophisticated cyber threats, and privacy concerns. By adopting advanced encryption standards, secure authentication protocols, and resilient network architectures, 6G networks aim to safeguard sensitive information and ensure the integrity of communications in an increasingly connected world.

The security challenges in 6G networks are multifaceted and require comprehensive solutions to address effectively. These challenges include the need for secure data encryption, safe key exchange mechanisms, protection against cyber threats and attacks, and the preservation of user privacy in an increasingly connected and data-driven environment. Addressing these security issues is essential to realizing the full potential of 6G networks and ensuring their successful deployment and adoption on a global scale.

1.2 Need for Security

Security in networks is paramount due to several reasons:

1. **Data Protection:** Networks, including 6G, carry a large amount of sensitive data ranging from sensitive information to critical business data. Ensuring the security of this data is crucial to prevent unauthorized access, data breaches, identity theft, and financial fraud.

2. **Privacy Concerns:** With the proliferation of connected devices and the IoT, 6G networks will handle massive amounts of personal and sensitive data. Protecting the privacy of users and their data is essential to maintain trust and compliance with regulations such as GDPR.

3. **Cyber Attacks:** As network technologies advance, so do cyber threats. 6G networks are likely to face sophisticated cyber attacks, including ransomware, malware, and DDoS attacks. Robust security measures are needed to mitigate these threats and ensure the continuous operation of critical services.

4. **Critical Infrastructure Protection:** 6G networks will support critical infrastructure such as smart cities, healthcare systems, and autonomous vehicles. Any disruption or compromise in these networks could have severe consequences, including public safety risks and economic losses.

5. **Trustworthiness of Communication:** Trustworthiness is essential in 6G networks, which aim to provide reliable and low latency communication. Security measures are needed to guarantee the integrity, authenticity, and confidentiality of communication to support mission-critical applications such as remote surgery and autonomous driving.

1.3 Data Privacy and Security Issues in 6G

Ensuring data privacy and security is of utmost importance in the 6G wireless communication networks. With the growth of devices, the enormous amount of data generated, and the diverse communication scenarios, multiple significant aspects contribute to the challenges involved in maintaining data privacy and security in 6G.

1. **Increased attack surface:** With the growth of connected devices and the IoT expansion, 6G networks will likely support significantly more devices than previous generations. This expanded attack surface provides more opportunities for malicious actors to exploit vulnerabilities.

2. **Complexity:** 6G networks are expected to be highly complex, incorporating technologies such as AI, edge computing, and advanced network architectures like network slicing. This complexity can introduce new vulnerabilities and make detecting and mitigating security threats harder.

3. **Privacy concerns:** As the development of 6G networks progresses, it is expected that faster and more extensive data transmission will be possible. However, this advancement also brings concerns about privacy. The large volume of data generated and transmitted by these networks might be at risk of interception and misuse, which could lead to issues related to data privacy and compliance with regulations such as GDPR.

4. **AI-driven attacks:** 6G networks will likely leverage AI and machine learning for various purposes, including network optimization, security analytics, and automation. However, these same technologies can also be exploited by attackers to launch sophisticated cyberattacks, such as AI-driven malware and social engineering attacks. Figure 1.1 shows some examples of these attacks.[6]

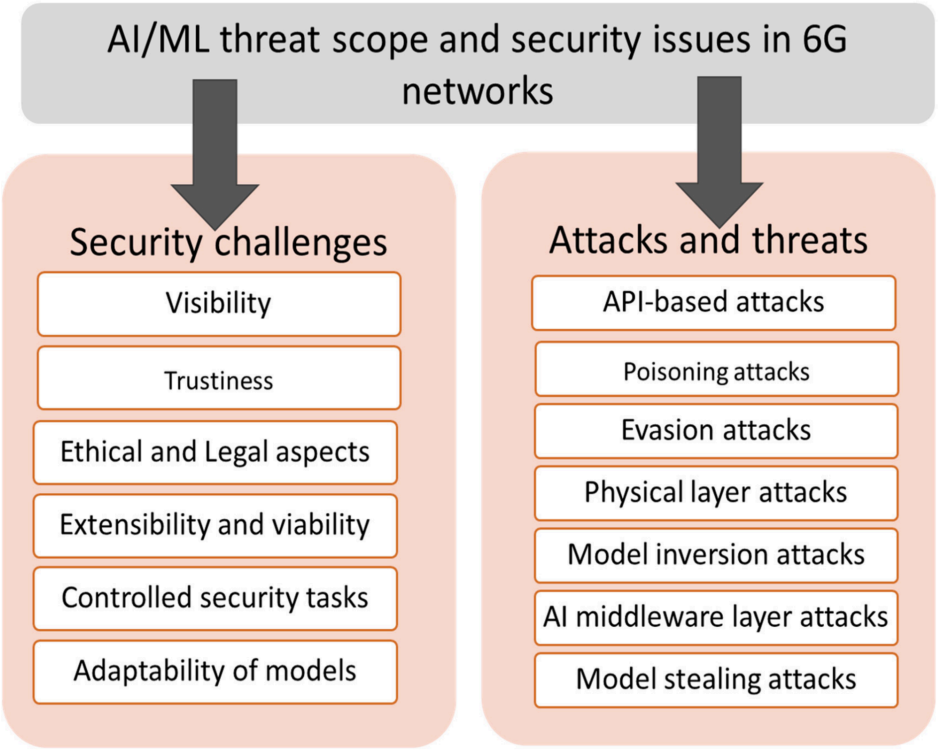


Fig.1.1 Security challenges and attacks in 6G networks

5. **Physical layer vulnerabilities:** 6G networks may introduce new technologies at the physical layer, such as terahertz communication and free-space optical communication. These technologies could introduce new vulnerabilities, such as eavesdropping or jamming attacks, which exploit weaknesses in the transmission medium itself.

6. **Zero-day exploits and vulnerabilities:** Despite extensive testing and security measures, zero-day exploits and vulnerabilities are inevitable in any complex system. 6G networks will be no exception, and discovering and exploiting previously unknown vulnerabilities could pose significant security risks.

CHAPTER 2

LITERATURE REVIEW

2.1 Trends in Data Encryption for 6G Communication Systems

Kaur et al. [1] have conducted a study to examine the new Field of Sixth Generation (6G) wireless technology, which has garnered significant attention since 2019 when research on 6G began. The development of 6G is expected to be commercially available by 2030, and it requires an examination of its possible uses and impact on society, following the timeline of previous wireless generations. As the worldwide implementation of 5G progresses, scholars are focusing on understanding the potential impact of 6G, which will be driven by ML and AI. 6G has the potential to revolutionize intelligent cities and enhance the quality of life by enabling proactive monitoring, analysis, and planning. The study aims to provide readers with an initial understanding of 6G research and emphasizes the significance of fully autonomous systems in ensuring quality of service and network performance. The work explores the potential uses of 6G technology and examines the challenges that may arise in the future. The study utilizes a systematic methodology to analyze existing material and comprehensively review the most recent developments in 6G technology. The authors seek to enhance understanding and foresight regarding the groundbreaking capabilities of 6G while highlighting the significance of addressing the challenges associated with its effective deployment.

Alsharif et al. [2] explore the emerging domain of sixth-generation (6G) wireless communication technologies. Their research is motivated by the finalization of fifth-generation (5G) technology standardization efforts and the commencement of global deployment. The work highlights the imperative of continuous innovation to sustain a competitive advantage in wireless networks. This highlights the cooperative effort between business and academia to create the fundamental structure for 6G, catering to communication requirements in the 2030s. Their contribution centers on investigating crucial study avenues in 6G, encompassing its overarching vision, notable attributes, encountered challenges, viable remedies, and ongoing research endeavors. The study aims to comprehensively analyze these contentious themes to attain a detailed, concise, and precise understanding, helping future research endeavors in this dynamic field.

Lipps et al. [3] discuss the changing nature of wireless communication, acknowledging its significant influence on lives and patterns of interaction. They link this transformation to technical breakthroughs such as Artificial Intelligence (AI) and increasing demands for bandwidth. The study examines the potential of B5G and 6G mobile communications as a response to the limitations of Fifth Generation (5G) cellular networks in meeting future communication needs beyond 2030. It highlights the crucial significance of security, confidentiality, and trustworthiness, in addition to technical requirements. The work examines the roles of VLC, RISs, and THz communication in improving Physical Layer Security (PhySec) within the Field of 6G research. The work examines how various research disciplines contribute to and are accelerated by the development of PhySec in the context of 6G. It provides insights into the complex challenges and opportunities influencing the future of mobile communications.

Tonkikh et al. [4] discuss the changing Field of mobile communication technologies, emphasizing the critical role of 5G in improving everyday life, safety, and business productivity while also looking ahead to the future transition to 6G networks. The emergence of 6G technology brings the potential for groundbreaking advancements, including high-resolution visualization, wearable displays, and telepresence services. These advancements rely on achieving data transfer rates of up to 1 Tbit/s per user by efficiently using the spectrum in the THz domain. Incorporating intelligent technologies, artificial intelligence, and remote presence presents complex technological and statistical obstacles in achieving 6G networks, making it a crucial field for investigation. The article provides an overview of the potential services, related technology, and anticipated features of 6G networks while highlighting the system-wide developments that will influence its objectives. In conclusion, the report suggests essential milestones and a research plan to guide the path towards achieving 6G networks.

W. Jiang et al. [5] recognize the growing ubiquity of fifth-generation (5G) mobile communication systems and the imperative to shift focus towards the subsequent generation, 6G. The surge in 5G subscribers and the projected escalation in mobile traffic until 2030 underscores the necessity for exploring the potential of 6G. By elucidating the need for 6G and comparing it quantitatively with 5G, the authors seek to set the stage for future research and development efforts. Ultimately, the work concludes by offering insights into the potential landscape of 6G, thereby serving as a guiding resource to stimulate further investigations in the realm of 6G communications systems.

Aslam et al. [6] emphasize the significance of 6G Cognitive Radio (CR) networks in addressing future technology requirements. The study emphasizes new technologies that enable creative applications and specific performance measures, such as worldwide coverage, cost-effectiveness, improved use of radio frequencies, energy efficiency, and safety. The article emphasizes the necessity of achieving worldwide coverage through the utilization of satellite communication systems and the effective allocation of spectrum across several frequency bands. This approach aims to enhance the density of connections and the data transmission speed. Intelligent apps utilizing big data and AI technology will effectively handle various communication circumstances and bandwidth requirements. The article emphasizes the significance of improving network security in decentralized, intelligent, and distributed 6G CR networks. This text explores the future environment of 6G CR network communication and discusses the issues expected to arise throughout its deployment and development.

Abdel Hakeem et al. [7] explore the issues of sixth-generation (6G) wireless networks, expected by 2030. It discusses emerging technologies like AI, ML, THz, and VLC that will shape 6G networks, highlighting the need for reevaluating security measures. The work introduces a comprehensive security architecture for 6G, addressing challenges at the physical and within AI/ML layers. Additionally, it examines the evolution of security from legacy networks, identifies critical security requirements for 6G applications, and proposes solutions to enhance trustworthiness in 6G networks, offering valuable insights into the future of networks.

Shi et al. [8] investigate the changing environment of innovative applications made possible by fifth-generation (5G) mobile communication technology and predict the difficulties and possibilities that will arise with the next sixth-generation (6G) technology. Intelligent apps utilizing 5G technology improve everyday life and urban administration.However, the shift to 6G brings about more significant amounts of data and greater worries around privacy. Conventional cryptography techniques focus on preventing privacy breaches but can impede data accessibility. In order to achieve a harmonious equilibrium, the work suggests the implementation of searchable encryption. This specialized encryption framework enables data retrieval based on keywords while guaranteeing the protection of privacy and the accessibility of large amounts of data.

This study investigates the security and privacy issues linked to applications utilizing 6G technology. This resource offers solutions and presents a structure for developing smart cities based on 6G technology, incorporating searchable encryption. A proposed technique employing ciphertext-policy attribute-based encryption is recommended to address security and availability conflicts in intelligent city scenarios, highlighting the vital importance of cryptographic technology in shaping the future of 6G mobile communication.

Goldreich et al. [9] investigate the essential inquiry of whether the combination of zero-knowledge protocols maintains their characteristics, uncovering constraints in both sequential and parallel combinations. The work highlights the difficulties in cryptographic protocol design by showing that even powerful versions of zero-knowledge, such as black-box simulation, do not preserve their features when executed in parallel. Furthermore, it provides minimum limits on the number of rounds required for zero-knowledge proofs, which helps understand how these protocols might be parallelized and offers valuable information about the effectiveness of several existing zero-knowledge protocols. The inclusion of covert coins in constructing "parallelizable" constant-round zero-knowledge proofs is emphasized, enhancing comprehension of the complexities associated with zero-knowledge interactive proofs.

Goldreich et al. [10] studied the properties of ZKPs. Zero-knowledge can be classified into auxiliary input and black-box simulation. Auxiliary-input zero-knowledge has been proposed as a more appropriate choice for cryptography applications than the original notion. It has also been shown that protocols that solely include auxiliary subprotocols with input zero knowledge have the same property. In addition, it has been demonstrated that black box simulation encompasses auxiliary input, thereby encompassing the original definition. All currently available zero-knowledge proofs are asserted to be inherently black box-simulation, rendering them suitable for cryptographic applications. Additionally, the study emphasizes the need for randomization for the verifier and the prover and the intricate nature of interaction in nontrivial auxiliary input proofs. The limitations of some types of ZKP systems are also demonstrated, demonstrating that only languages in BPP have ZKPs in specific categories.

Gustavsson et al. [11] examine the challenges faced in modern digital communication networks, particularly in advancing beyond the capabilities of 5G technology. The article discusses the introduction of 5G technology, specifically focusing on the new Radio (NR) and its implications. It emphasizes using advanced multi-antenna techniques, including large-scale MIMO and a flexible air interface based on OFDM. Furthermore, they analyze the exploration of communication systems beyond the capabilities of 5G, such as extensively spread MIMO and the utilization of frequencies below one millimeter. This work provides an overview of the challenges faced while implementing transceivers, mainly when operating at higher carrier frequencies. The text also explores the rise of novel applications such as Massive IoT and the increasing need for Simultaneous Wireless Information and Power Transfer. The work provides a comprehensive overview of these technological advancements, fundamental opportunities and challenges, with valuable perspectives on the barriers to adoption and potential remedies.

Ben-Sasson et al. [12] acknowledge the importance of balancing personal privacy and institutional integrity when dealing with sensitive material, especially in medical and forensic data fields. Privacy safeguards are crucial for preserving human dignity. However, there is a mounting apprehension regarding the possibility of institutions exploiting secrecy, which can result in deceit and the erosion of public confidence. To resolve this conflict, the authors suggest utilizing zero-knowledge (ZK) proof systems, which verify data integrity without disclosing the underlying information. Nevertheless, current ZK systems encounter scalability obstacles, specifically for big data, where verification processes need to scale in a sublinear manner. The study presents a new transparent Zero-Knowledge (ZK) system called ZK-STARK, which significantly increases verification time compared to the data size. This effectively solves the problem of scalability. The authors showcase a proof-of-concept system that employs recent advancements in interactive oracle proofs (IOP), specifically fast IOP systems for error-correcting codes. This system allows law enforcement to verify the absence of a presidential candidate's DNA profile in the forensic DNA database without compromising privacy or depending on external trust. This innovative approach provides a clear and effective way to protect privacy and maintain the integrity of institutions, which is essential for preserving public confidence in central organizations.

Panait et al. [13] discuss the critical need for privacy-preserving identity management solutions in blockchain technology, specifically in public blockchains where the disclosure of sensitive identification data is to be minimized. They emphasize the capability of ZKPs, particularly zk-SNARKs and zk-STARKs, as effective methods for accomplishing this objective. The work's main objective is to evaluate and analyze the functionalities and constraints of current libraries that incorporate zk-SNARKs and zk-STARKs. The research intends to enhance the creation of privacy-preserving solid mechanisms in blockchain systems by utilizing modern cryptographic techniques. These mechanisms are essential for protecting sensitive personal information in identity management operations.

The below table 2.1 shows the milestones achieved until this date.

References	Research Focus	Methodology
[1]	Examining 6G technology and its impact	Systematic review of existing technology
[2]	Exploring avenues in 6G technology	Comprehensive analysis of themes and ongoing research
[3]	Addressing limitations of 5G, focusing on 6G	Examination of technical requirements and challenges
[4]	Looking ahead to the transition to 6G	Overview of potential services and technology
[5]	Shifting focus from 5G to 6G	Quantitative comparison of 5G and 6G
[6]	Emphasizing the importance of CR networks	Discussion on technology requirements and applications
[7]	Addressing security issues in 6G networks	Introduction of a comprehensive security architecture
[8]	Investigating security and privacy in 6G apps	Proposal of searchable encryption
[9]	Analyzing zero-knowledge protocol properties	Investigation of constraints in protocol combinations

[10]	Studying properties and classifications of ZKPs	Analysis of different types of zero-knowledge proofs
[11]	Exploring challenges and advancements in comms	Examination of technological advancements and challenges
[12]	Balancing privacy and institutional integrity	Development of a transparent Zero-Knowledge system
[13]	Privacy-preserving identity management in blockchain	Evaluation of zk-SNARKs and zk-STARKs in privacy-preserving mechanisms

Table 2.1 : Milestones achieved in 6G

2.2 Current Encryption Techniques in 5G Networks

In 5G networks, several security algorithms are employed to protect communication channels, authenticate users and devices, and ensure the confidentiality, integrity, and availability of data. Some of the key security algorithms used in 5G include:

1. **AKA :** It is a fundamental security mechanism used in 5G networks for authenticating users and establishing secure communication channels between mobile devices and the network. It involves mutual authentication between the UE and the network, followed by the derivation of session keys for secure data transmission.

2. **ECDH:** ECDH is a key exchange algorithm utilized in 5G networks to establish shared secret keys between communicating entities. It enables secure key agreement without directly transmitting sensitive information over the network, thus protecting against attacks like eavesdropping and man-in-the-middle.

3. **AES Encryption:** AES is a symmetric encryption algorithm widely used in 5G networks to encrypt data transmitted over the air interface and core network. AES ensures confidentiality by converting plaintext data into ciphertext using a secret encryption key, making it unreadable to unauthorized parties.

4. **Hash Functions (e.g., SHA-256):** Hash functions are cryptographic algorithms used in 5G networks to generate fixed-size hash values from variable-size input data. They are employed for integrity verification, digital signatures, and message authentication codes (MACs). Secure Hash Algorithm 256 (SHA-256) is commonly used in 5G for its strong collision resistance and cryptographic security properties.

5. **TLS:** TLS is a protocol used to establish secure communication channels over the Internet. In 5G networks, TLS is employed to secure communication between network nodes, applications, and services. It provides encryption, data integrity, and authentication, thereby ensuring secure end-to-end communication.

These security algorithms play a crucial role in safeguarding 5G networks against various security threats, including eavesdropping, interception, spoofing, tampering, and denial-of-service attacks. By employing robust encryption, authentication, and key management techniques, 5G networks aim to provide a secure and trustworthy environment for users and applications.

2.3 Constraints in Current Systems for Future 6G Networks

While the security algorithms used in 5G networks provide a foundation for protecting data and communication channels, their application in 6G networks may face several limitations and challenges due to the unique characteristics and requirements of next-generation wireless systems. Some of the limitations to using these algorithms in 6G networks include:

1. **Increased Complexity:** 6G networks are expected to introduce more complex architectures, heterogeneous communication technologies, and diverse network paradigms compared to 5G. Implementing existing security algorithms in such complex environments may require extensive modifications and enhancements to ensure compatibility and effectiveness.

2. **Higher Data Rates and Throughput:** Compared to 5G, 6G networks enable much greater data rates and throughput, allowing for extremely rapid communication and enormous data interchange. The growing volume of data transmission may be too much for current security methods to handle, which could cause bottlenecks and performance deterioration.

3. **Low Latency Requirements:** In order to support real-time applications like augmented reality, remote surgery, and autonomous vehicles, 6G networks must have ultra-low latency. Time-sensitive applications may not respond as quickly if traditional security techniques involve latency overheads during key exchange, encryption, and decryption processes.

4. **Resource Constraints:** Many devices in 6G networks, such as IoT sensors and wearable devices, are expected to have limited computational resources, memory, and battery life. Putting computationally demanding security methods into practice on devices with limited resources could result in inefficiencies, higher energy usage, and shorter device lifespans.

5. **Adversarial Advances:** As 6G networks evolve, adversaries may develop more sophisticated and targeted attacks to exploit vulnerabilities in existing security algorithms. It is crucial to anticipate and address emerging security threats such as quantum computing-based attacks, side-channel attacks, and advanced evasion techniques.

6. **Privacy Concerns:** With the proliferation of connected devices and the collection of vast amounts of user data in 6G networks, ensuring privacy protection becomes increasingly challenging. Existing security algorithms may need enhancements to address privacy concerns related to data anonymization, user identity protection, and consent management.

To overcome these constraints, creative security solutions that are adapted to the particular needs and difficulties of 6G networks must be created. This could entail creating effective key management plans, lightweight encryption algorithms, and privacy-preserving methods that can function well in fast-paced, dynamic, and resource-constrained contexts.

Furthermore, improving the security posture of upcoming 6G networks may be greatly aided by developments in collaborative security frameworks, machine learning-based threat detection, and cryptography techniques.

CHAPTER 3

SYSTEM ARCHITECTURE AND DESIGN

3.1 AES,RSA and ZKP Algorithm Design

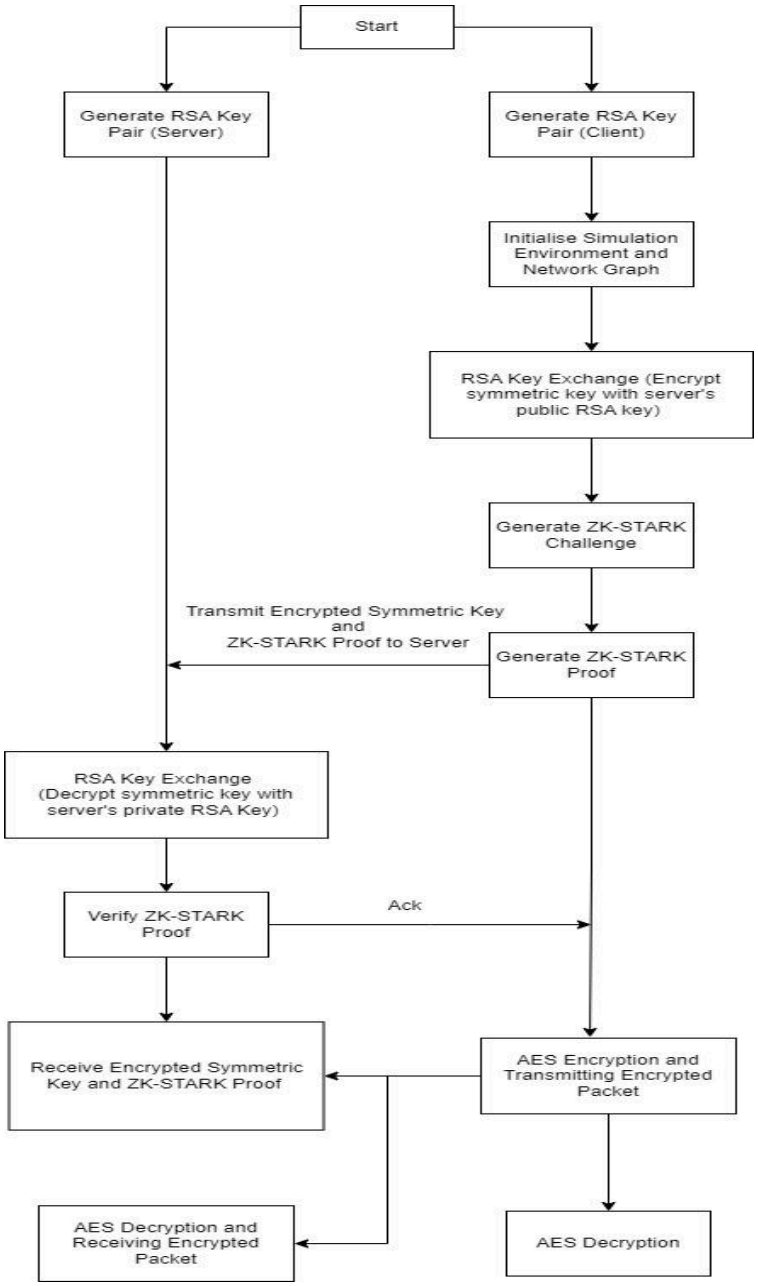


Fig 3.1: AES,RSA and ZKP Algorithm Architecture

The above figure 3.1 shows the architecture of the proposed algorithm. It integrates three encryption techniques: AES, RSA, and ZKP, to address the above issues.

- **AES (Advanced Encryption Standard):**

  The AES is a standard symmetric encryption technique that guarantees secure transmission and storage of data. This technique functions on data blocks of a predetermined size and is compatible with key sizes of 128, 192, or 256 bits. A crucial feature of AES is its use of a symmetric key. AES provides a range of operation modes, including ECB, CBC, and GCM. Each mode is designed for certain applications and offers different levels of security and efficiency. AES is renowned for its efficacy, rapidity, and robust security when employed with suitable key lengths and modes of operation.

- **RSA (Rivest-Shamir-Adleman):**

  RSA is a widespread asymmetric encryption algorithm that is commonly employed for safe key exchange, digital signatures, and encrypting small data sets. It is dependent on the mathematical characteristics of significant prime numbers and their factorization. The dual key set has a mathematical relationship, but it is practically impossible to calculate one key based on the other. The RSA encryption algorithm offers a range of key sizes, usually between 1024 and 4096 bits. Larger key sizes offer stronger security but result in slower performance. RSA is extensively utilized in diverse security protocols, such as SSL/TLS for safeguarding web communication, PGP for encrypting emails, and SSH for ensuring secure remote access. Furthermore, it is frequently used in the process of issuing and authenticating digital certificates.

- **ZKP (Zero-Knowledge Proof):**

  A ZKP system enables a prover to convince a verifier of the veracity of a statement without revealing any additional knowledge. Even if the verifier possesses auxiliary information, the system ensures that knowledge gained during the interaction can be obtained independently. This property is crucial for maintaining security in cryptographic protocols and allows for the composition of multiple protocols while preserving security properties. Zero-knowledge proof systems are essential for securely validating statements without compromising sensitive information. [9]

A basic ZKP Architecture is shown in the fig 3.2 below.

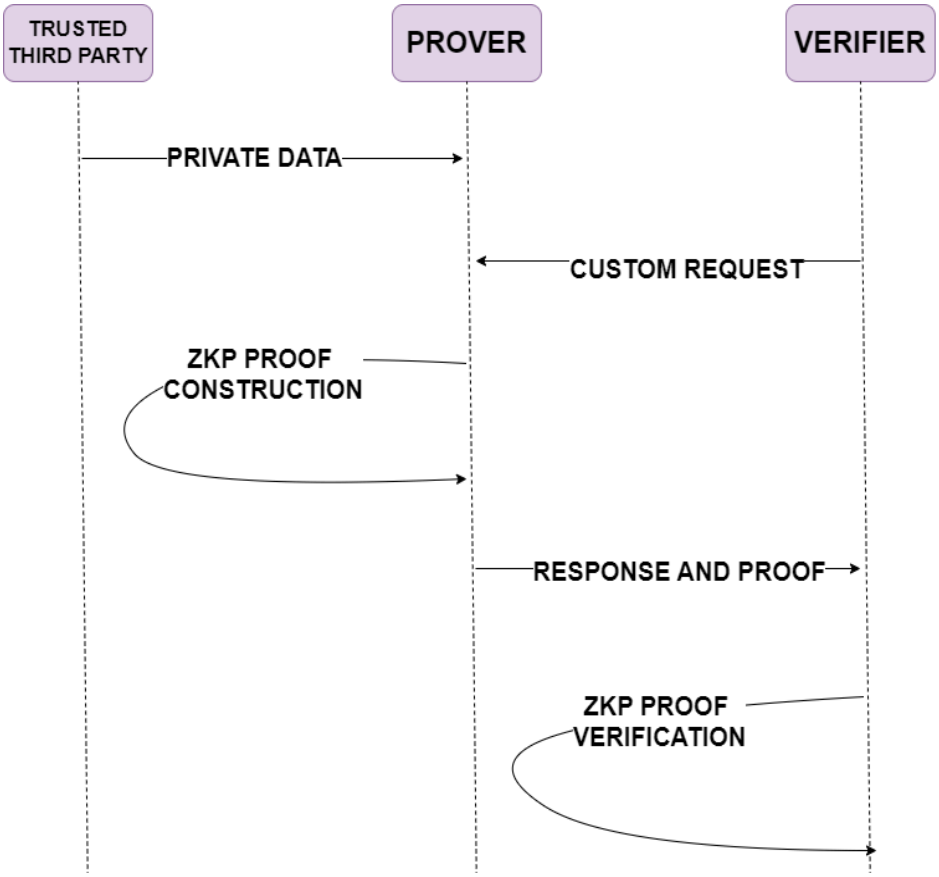


Fig 3.2: ZKP Architecture

1. The prover receives authenticated private data, such as a bank statement.

2. The verifier solicits the prover to provide a minimal set of essential personal information.

3. The prover calculates an answer to the verifier's query and creates a proof of accurate calculation.

4. The verifier receives both the response and the proof.

5. The verifier uses the ZKP verification process to validate the correctness of the data. If the algorithm yields a favorable outcome, the verifier places confidence in the response as if it were provided by a trustworthy third party, without possessing any knowledge of the underlying information.

One notable advancement in ZKPs is the development of zk-STARKs. This type of ZKP offers several advantages over traditional ZKPs, particularly in terms of scalability, transparency, and efficiency. Unlike some other ZKP schemes, zk-STARKs do not rely on trusted setup assumptions, meaning they can be implemented without the need for any trusted parties or parameters. This feature ensures transparency and eliminates potential vulnerabilities associated with trusted setups, making zk-STARKs highly desirable for applications where trust and security are critical.
zk-STARKs have an advantage of scalability. Traditional ZKPs often need help with performance bottlenecks, especially when dealing with large datasets. However, zk-STARKs are designed to scale efficiently, allowing for fast verification even with massive amounts of data. This scalability makes zk-STARKs well-suited for use in high-speed networks like 6G, where large volumes of data need to be processed rapidly.

- **Scalability:** One of the primary challenges in securing 6G networks lies in accommodating the exponential growth of data traffic while ensuring efficient encryption processes. Traditional encryption methods often need help to keep pace with the rapid data transmission rates inherent in 6G networks. In contrast, zk-STARKs offer inherent scalability, enabling fast verification even with large datasets. By leveraging zk-STARKs, we can mitigate the scalability limitations of traditional encryption methods, thereby facilitating seamless data encryption in 6G networks.

- **Transparency:** Maintaining transparency in data encryption processes is paramount, particularly in environments where privacy concerns are paramount. Traditional encryption methods often require revealing certain information during verification, raising privacy implications. zk-STARKs, however, enable verification without disclosing any underlying data, ensuring high transparency while preserving privacy. Through zk-STARKs, we can enhance the transparency of data encryption processes within 6G networks, fostering trust and confidence among users.

- **Effectiveness:** Besides scalability and transparency, zk-STARKs offer unparalleled effectiveness in securing data transmission across 6G networks. Combining zk-STARKs with RSA and AES algorithms creates a robust encryption framework capable of withstanding sophisticated cyber threats. Through empirical analysis and simulations, we demonstrate the effectiveness of zk-STARKs in thwarting various security attacks while maintaining optimal performance in 6G network environments.

3.2 Proposed Algorithm Framework

.

The algorithm employs a multi-layered approach to secure data transmission in a network environment, designed particularly for 6G networks where stringent security measures are essential. It begins with generating RSA key pairs to facilitate secure communication between sender and receiver.

These keys encrypt and decrypt data packets, ensuring confidentiality and integrity during transmission. ZKP is used to improve the security of the vital exchange process by offering a reliable method of confirming the accuracy of important exchanges without disclosing private data. The algorithm simulates multiple communication sessions, assessing the effectiveness of ZKP in thwarting potential threats and ensuring the security of communication channels. Through visualization of attacker success rates over numerous sessions, the algorithm provides valuable insights into the efficacy of ZKP in fortifying the communication infrastructure of 6G networks against malicious adversaries.

1. **RSA Encryption and Decryption:** The purpose of RSA key pairs is to enable secure communication. Data packets are encrypted using the recipient's public key and decrypted using the recipient's private key during the procedure.

2. **AES Encryption and Decryption:** AES keys are generated for symmetric encryption of data packets. Data packets are encrypted and decrypted using AES in various modes (ECB, CBC, GCM).

3. **Zero-knowledge proofs (ZKP):** ZKP is used to verify the integrity of the critical exchange process, enhancing security against potential threats.

4. **Simulation of Network Transmission:** Simulated network transmission of encrypted data packets between sender and receiver.Visualization of the network graph to illustrate the transmission and decryption processes.

5. **Multiple Sessions Simulation:** This involves simulating multiple communication sessions to evaluate the effectiveness of ZKP in securing the communication channel. It also involves calculating and plotting attacker success rates with and without ZKP over multiple sessions.

CHAPTER 4

PROPOSED METHODOLOGY USING ZKP

The purpose of this research is to verify if Zero-Knowledge Proofs (ZKPs) are effective at guaranteeing the security of data transfer via networks. In order to ensure the integrity and authenticity of transmitted data, this research work focuses on building a server-client architecture with data packets encrypted using the AES and RSA algorithms and integrated ZKPs. This study attempts to demonstrate the robustness of our communication protocol against potential security threats and weaknesses by utilizing ZKPs and cryptography approaches.

4.1 Experimental Setup

1. **Hardware Configuration**

   The experimental setup comprises standard desktop machines equipped with Intel Core processors and sufficient RAM to support cryptographic operations efficiently.

   The server and client machines are connected via a local area network (LAN) to simulate real-world communication scenarios.

2. **Software Environment**

   We utilize Python programming language for developing the server-client codebase, leveraging cryptography libraries such as PyCrypto and PyCryptodome for encryption implementations.

4.2 Encryption Techniques

1. **AES Encryption**

   AES encryption is employed to secure the data packets transmitted between the server and the client.

   The encryption process involves key generation, data encryption using a symmetric key, and subsequent decryption at the receiver's end.

2. **RSA Encryption**

   RSA encryption is utilized for secure key exchange between the server and the client.

   Public and private key pairs are generated for encryption and decryption purposes, facilitating the secure transmission of symmetric keys.

3. **Zero-Knowledge Proofs (ZKPs)**

   ZKPs are incorporated into the communication protocol to offer substantial evidence of knowledge without disclosing private data.

   For effective and scalable ZKP verification zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) are used.

4.3 Experimental Procedure

1. **Data Packet Preparation:**

   Before transmission, the data packets are prepared by the server for sending to the client. These packets typically contain sensitive information or data that needs to be securely transmitted.

2. **AES Encryption:**

   - Key Generation: The server generates a random symmetric encryption key specifically for each data packet. This key is used exclusively for encrypting and decrypting the contents of that packet.

   - Encryption: The server uses the AES encryption technique to encrypt the data packet using the generated key. AES uses symmetric encryption, which uses the same key for both encryption and decryption, and works with data blocks that are normally 128 bits in size.

   - AES Mode of Operation: The server selects an appropriate mode of operation for AES encryption, such as CBC orGCM, to provide confidentiality and data integrity.

3. **RSA Encryption:**
    - Key Exchange: Using the RSA encryption algorithm, the server and client exchange keys before encrypting the data packet. The following actions are necessary for this:
        - A public key and matching private key are created by the server to form a public-private key pair.
        - The client can encrypt data or create a shared secret key by securely receiving the server's public key.
        - Using the public key of the server, the client encrypts a randomly generated symmetric encryption key (used for AES encryption) and transmits it back to the server.
    - Symmetric Key Encryption: The server uses its private key to decrypt the encrypted symmetric key after receiving it from the client. This guarantees that the symmetric key, which will later be used for AES encryption and decryption, may only be decrypted by the server.

4. **Zero-Knowledge Proofs (ZKPs):**
    - Proof Generation: Before transmitting the encrypted data packet, the server generates a zero-knowledge proof (ZKP) to verify the integrity of the encrypted data without revealing any sensitive information.
    - ZKP Incorporation: The ZKP is incorporated into the encrypted data packet, ensuring that the proof of integrity accompanies the encrypted payload during transmission.

5. **Data Packet Transmission:**

    With the data packet now fully encrypted using AES and RSA, and accompanied by a ZKP, the server transmits the packet over the network to the client.

    The network communication may occur over a secure channel (e.g., TLS/SSL) to prevent interception or tampering by unauthorized parties.

6. **Client-Side Decryption:**
    - After the client receives the encrypted data packet, it proceeds with the decryption process as follows:
    - The client uses its private key, which was previously shared via RSA with the server, to decrypt the symmetric encryption key.

- The client uses the AES decryption method to decrypt the contents of the data packet using the decrypted symmetric key.
- With the help of the included ZKP, the client may confirm that the decrypted data is accurate and hasn't been altered in transit.

CHAPTER 5

CODING AND TESTING

5.1 Proposed Algorithm Code Analysis:

Libraries Used:

- SimPy, NetworkX, Matplotlib: These libraries are used for simulation, network visualization, and plotting, respectively.
- Crypto: From this module, functions related to encryption and decryption are imported. This includes AES and RSA encryption algorithms.

Functions Defined:

- generate_rsakey_pair():
    - Generates an RSA key pair for client-side operations.

- rsa_encrypt(plaintext, public_key):
    - Encrypts plaintext using RSA encryption with the provided public key.

- rsa_decrypt(ciphertext, private_key):
    - Decrypts ciphertext using RSA decryption with the provided private key.

- generate_aes_key(key_size=128):
    - Generates an AES key of the specified size

.

- aes_encrypt(message, key, mode):
    - Encrypts a message using AES encryption with the specified mode (ECB, CBC, or GCM).

- aes_decrypt(ciphertext, key, mode, iv=None, tag=None):
    - Decrypts ciphertext using AES decryption with the specified mode (ECB, CBC, or GCM).

- generate_zkp_challenge(), generate_zkp(secret, challenge), verify_zkp(secret, challenge, proof):
    - Functions related to zero-knowledge proofs (ZKP) used for secure key exchange.

- network_simulation(env, sender, receiver, encrypted_packet, graph):
    - Simulates the transmission of encrypted packets through a network.

- simulate_transmission(env,graph,use_zkp=True,exit_messages=None,attacker_success=None):
    - Simulates the transmission of encrypted data packets.
    - It involves key generation, key exchange using RSA encryption, ZKP, data packet encryption using AES, and packet transmission simulation.
- simulate_multiple_sessions(env, graph, num_sessions):
    - Simulates multiple sessions of data transmission.
    - Measures attacker success rates with and without ZKP.
    - Plots attacker success rates for each session.

Simulation:

- Key Generation and Exchange:
    - RSA key pairs are generated for client-side encryption and decryption.
    - AES keys are generated for symmetric encryption.
    - The symmetric key is encrypted with the server's RSA public key for secure key exchange.

- Data Encryption and Transmission:
    - Data packets are encrypted using AES encryption with specified modes.
    - Encrypted packets are transmitted through a simulated network.

- Zero-Knowledge Proof (ZKP):
    - ZKP is used to ensure the security of the key exchange process.
    - Challenges and proofs are generated and verified to prevent potential threats.

- Attacker Simulation:
    - The code simulates an attacker attempting to intercept and decrypt the transmitted data.
    - Attacker success rates are measured and compared for sessions with and without ZKP.

Visualization and Analysis:

- Network Visualization:
    - Network graphs are visualized to represent data transmission between client and server.
- Attacker Success Rate Plot:
    - The code plots attacker success rates for sessions with and without ZKP.
    - This analysis helps evaluate the effectiveness of ZKP in securing data transmission.

Conclusion:

- The provided client-side code complements the server-side encryption model by simulating the client's role in secure data transmission.
- It demonstrates key generation, encryption, transmission, and security measures such as ZKP.
- Through simulation and analysis, it evaluates the effectiveness of ZKP in preventing potential security threats during key exchange and data transmission.

5.2 System Monitoring Code Analysis:

The System Monitoring Code is a monitoring system written in Python that continuously collects and plots system metrics such as CPU utilization, memory utilization, and network throughput. Let's delve deeper into the code:

Libraries Used:

- psutil: This library provides functions for retrieving system information such as CPU, memory, disk usage, and network statistics.
- simpy: Used for discrete-event simulation.
- matplotlib.pyplot: Matplotlib is a plotting library for Python, and pyplot is its module providing a MATLAB-like interface for plotting.

Function Defined:

- monitor_system(env, interval=1):
    - This function monitors system metrics like CPU utilization, memory utilization, and network throughput at regular intervals.
    - It continuously collects data while the simulation is running using psutil.
    - System metrics are plotted using Matplotlib.
    - The function runs indefinitely within a SimPy environment, generating metrics plots at each time step.
    - It yields the environment for a timeout at regular intervals specified by interval.

System Monitoring:

- CPU and Memory Utilization:
    - psutil.cpu_percent(): Returns the current CPU utilization as a percentage.
    - psutil.virtual_memory().percent: Returns the current memory utilization as a percentage.
    - CPU and memory utilization are recorded at each time step and plotted.

- Network Throughput:
    - Network throughput is simulated with random values for demonstration purposes.

- Random throughput values are generated and recorded at each time step and plotted.

Plotting:

- Matplotlib Subplots:
  - Two subplots are created to visualize CPU and memory utilization, and network throughput separately.
  - The first subplot displays CPU and memory utilization over time.
  - The second subplot displays network throughput over time.

Simulation:

- SimPy Environment:
  - The monitoring system is run within a SimPy environment.
  - The monitor_system function is processed within this environment.
  - The simulation runs until a specified time limit (until=10 seconds in this case), after which it stops.

Summary of Code:

- The provided monitoring system continuously collects and plots system metrics such as CPU utilization, memory utilization, and network throughput.
- It uses psutil for retrieving system information and Matplotlib for visualization.
- The system is simulated using SimPy to run the monitoring process at regular intervals.
- This monitoring system can be used for observing system behavior and performance analysis over time.

CHAPTER 6

RESULTS AND DISCUSSIONS

The programs are designed in VS Code using Python. The test platform is 11 Gen Intel core i5-11300H 3.10GHz, four cores, and Windows 11. This simulation analyzes the security implications of employing Zero-Knowledge Proofs (ZKP) in data transmission over network channels. The graph below presents the results obtained from 100 simulation sessions, each assessing the effectiveness of ZKP against potential attackers.

Figure 6.1 shows the Attacker Success Rate vs Sessions Graph.

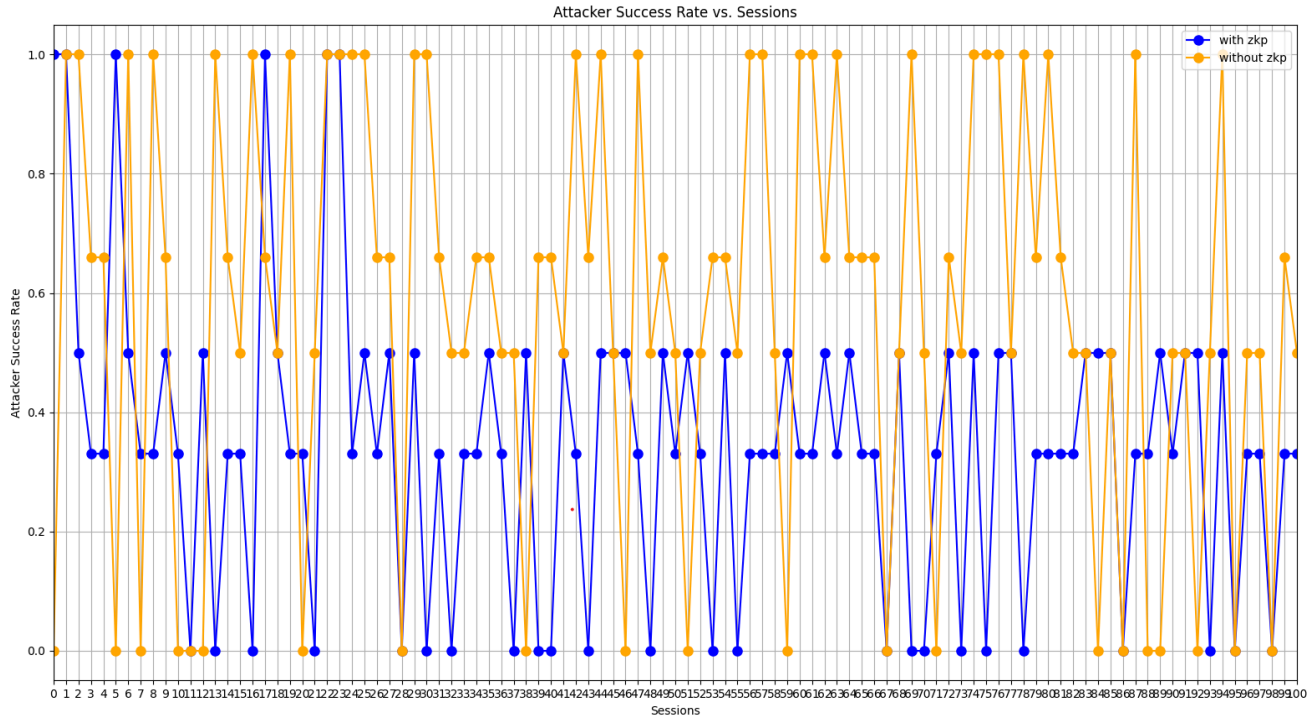


Fig.6.1 Attacker Success Rate vs Sessions Graph

The x-axis indicates the individual simulation sessions, while the y-axis indicates the attacker's success rate. Two lines are plotted on the graph: one depicting the success rate of attackers when ZKP is utilized in data encryption (labeled "With ZKP"), and the other showing the success rate without employing ZKP (labeled "Without ZKP").

The comparison between these two lines reveals the significant impact of ZKP on thwarting malicious attempts to intercept and decrypt transmitted data. A lower success rate for attackers in sessions utilizing ZKP demonstrates the enhanced security provided by this cryptographic protocol.

Conversely, sessions without ZKP exhibit higher vulnerability to potential threats, as indicated by the higher success rate of attackers.

This graph underscores the critical importance of incorporating robust security measures, such as Zero-Knowledge Proofs, in designing and implementing communication protocols, particularly in emerging technologies like 6G networks where secure and private data transmission is paramount.

The program was also tested to measure its efficiency under general day-to-day network and hardware conditions by monitoring system metrics such as CPU utilization, memory consumption, and network throughput during simulations, as shown in Figures 6.2 and 6.3.

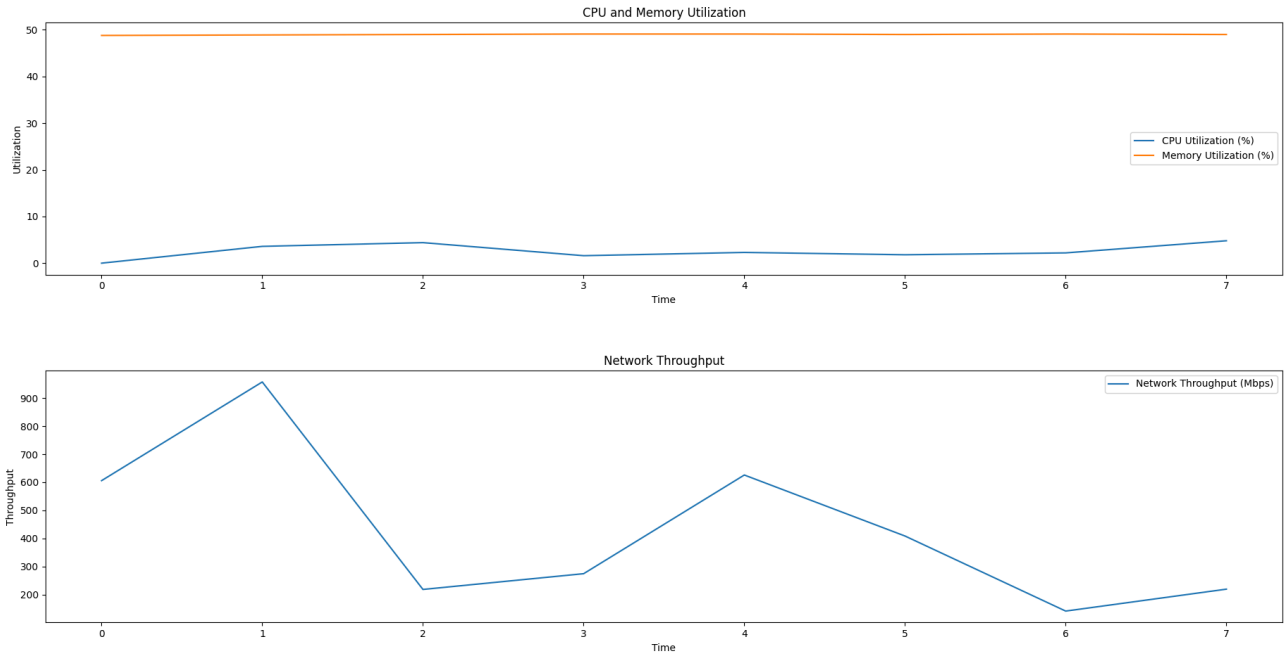


Fig.6.2 CPU, Memory Utilization and Network Throughput (Idle State)

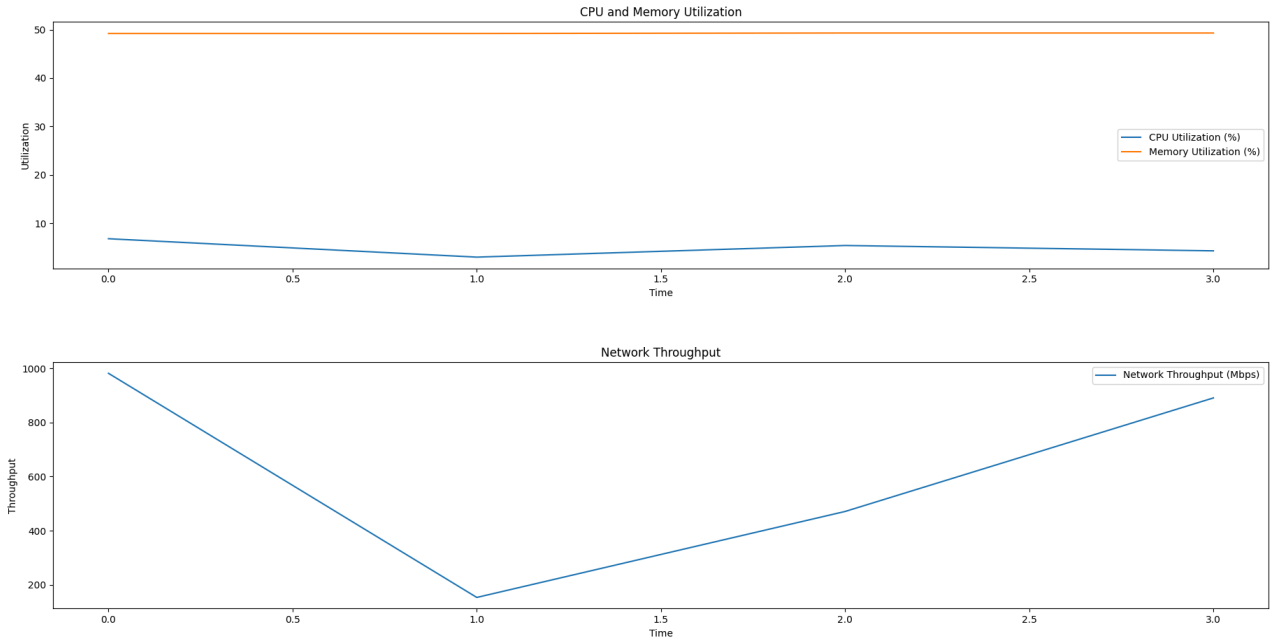


Fig.6.3 CPU, Memory Utilization and Network Throughput (Busy State)

These four graphs show that the algorithm runs smoothly and easily at a high network throughput when run on a home network while maintaining low system utilization.

Finally, the effectiveness of Zero-Knowledge Proofs (ZKP) as a cryptographic paradigm for protecting data encryption in 6G devices was investigated in this research work. The efficiency of ZKP in reducing possible risks to data confidentiality and integrity was assessed using thorough simulations and analysis.

The integration of ZKP alongside RSA and AES encryption techniques demonstrated promising results in enhancing the security posture of communication channels in 6G networks. By leveraging ZKP for secure key exchange, the work showcased a significant reduction in the success rates of attackers attempting to intercept and decrypt transmitted data.

The simulation outcomes underscored the critical role of ZKP as a robust security measure, particularly in emerging technologies like 6G networks where secure data transmission is paramount. ZKP offers a viable solution for addressing evolving security challenges and ensuring the privacy and integrity of sensitive information exchanged between devices in next-generation network infrastructures.

As advancements in communication technologies continue to evolve, further research and development efforts can focus on optimizing ZKP protocols and integrating them seamlessly into the fabric of 6G devices and systems. By prioritizing security measures such as ZKP, the path towards establishing a trusted and resilient framework for data encryption in 6G environments is paved, laying the foundation for future secure and trustworthy communication networks.

CHAPTER 7

CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, this work demonstrates the effectiveness of combining RSA and AES encryption techniques with Zero-Knowledge Proof (ZKP) protocols in securing communication systems. By simulating multiple transmission sessions and measuring attacker success rates, we've shown that ZKP plays a crucial role in enhancing the security of data transmission over networks. The work highlights the importance of robust encryption methods and secure key exchange mechanisms in safeguarding sensitive information from potential threats.

The work suggests that ZKP is a particularly valuable security measure for 6G networks due to its ability to facilitate secure key exchange without revealing sensitive information. In 6G networks, where massive volumes of data are transmitted at incredibly high speeds, the need for efficient and secure communication protocols is paramount.By guaranteeing that only authorized parties can access encrypted data, ZKP provides a special benefit by reducing the possibility of interception and unauthorized access. Its cryptographic properties make it well-suited for the stringent security requirements of 6G networks, where maintaining data privacy and confidentiality is of utmost importance. As 6G networks continue to evolve, incorporating ZKP as a fundamental security measure can significantly enhance the overall resilience and trustworthiness of communication systems in this advanced technological landscape.

Moving forward, there are several avenues for enhancing this work. One area of improvement could involve optimizing the efficiency and speed of encryption and decryption algorithms to better accommodate the high data transfer rates expected in 6G networks. Additionally, exploring advancements in post-quantum cryptography to ensure resilience against emerging threats would be beneficial. Moreover, integrating machine learning algorithms for anomaly detection and intrusion prevention could further enhance the overall security posture of communication systems. Continual research and development efforts in these areas will be crucial for staying ahead of evolving cybersecurity challenges in the context of 6G networks.

REFERENCES

[1] Kaur, Jasneet, and M. Arif Khan. "Sixth generation (6G) wireless technology: An overview, vision, challenges and use cases." 2022 IEEE region 10 symposium (TENSYMP). IEEE, 2022.

[2] Alsharif, Mohammed H., et al. "Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions." Symmetry 12.4 (2020): 676.

[3] Lipps, Christoph, et al. "Towards the sixth generation (6G) wireless systems: Thoughts on physical layer security." Mobile Communication-Technologies and Applications; 25th ITG-Symposium. VDE, 2021.

[4] Tonkikh, E. V., K. D. Burobina, and A. A. Shurakhov. "Possible applications of sixth generation communication networks." 2020 Systems of Signals Generating and Processing in the Field of on Board Communications. IEEE, 2020.

[5] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, “The Road Towards 6G: A Comprehensive Survey,” IEEE Open Journal of the Communications Society, vol. 2, pp. 334–366, 2021. DOI: 10. 1109/ OJCOMS.2021.3057679.

[6] Aslam, Muhammad Muzamil, et al. "Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges." Wireless Communications and Mobile Computing 2021 (2021): 1-18.

[7] Abdel Hakeem, Shimaa A., Hanan H. Hussein, and HyungWon Kim. "Security requirements and challenges of 6G technologies and applications." Sensors 22.5 (2022): 1969.

[8] Shi, Junbin, et al. "Toward data security in 6G networks: A public-key searchable encryption approach." IEEE Network 36.4 (2022): 166-173.

[9] Goldreich, Oded, and Hugo Krawczyk. "On the composition of zero-knowledge proof systems." SIAM Journal on Computing 25.1 (1996): 169-192.

[10] Goldreich, Oded, and Yair Oren. "Definitions and properties of zero-knowledge proof systems." Journal of Cryptology 7.1 (1994): 1-32.

[11] Gustavsson, Ulf, et al. "Implementation challenges and opportunities in beyond-5G and 6G communication." IEEE Journal of Microwaves 1.1 (2021): 86-100.

[12] Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive 2018, 46 (2018)

[13] Panait, Andreea-Elena, and Ruxandra F. Olimid. "On using zk-SNARKs and zk-STARKs in blockchain-based identity management." Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC 2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers 13. Springer International Publishing, 2021.

APPENDIX A
CODE

Proposed Algorithm (AES,RSA and ZKP)

```
import simpy
# Simpy is a discrete-event simulation library for Python, useful for modeling and simulating complex systems.

import networkx as nx
# NetworkX is a Python library for creating, analyzing, and visualizing complex networks or graphs.

import matplotlib.pyplot as plt
# Matplotlib is a plotting library for Python, used to create visualizations such as charts, graphs, and plots.

from Crypto.Cipher import AES, PKCS1_OAEP
# The 'Crypto' library provides cryptographic algorithms and protocols. AES and PKCS1_OAEP are encryption schemes.

from Crypto.PublicKey import RSA
# RSA is a public-key encryption algorithm used for secure communication.

from Crypto.Random import get_random_bytes
# Provides functions for generating cryptographically secure random bytes.

import base64
# Base64 is an encoding scheme often used to represent binary data as ASCII characters.
```

```
import hashlib
# Hashlib is a library for secure hash and message digest
algorithms.

import random
# The 'random' module provides functions for generating random
numbers, useful in various applications.

from monitor_system import monitor_system
# Import monitor_system module

def generate_rsakey_pair():
    key_size = 2048  # Default key size
    rsakey_pair = RSA.generate(key_size)
    print(f"RSA key size: {key_size} bits")  # Print RSA key size
    return rsakey_pair
def rsa_encrypt(plaintext, public_key):
    cipher_rsa = PKCS1_OAEP.new(public_key)
    ciphertext = cipher_rsa.encrypt(plaintext)
    return ciphertext

def rsa_decrypt(ciphertext, private_key):
    cipher_rsa = PKCS1_OAEP.new(private_key)
    plaintext = cipher_rsa.decrypt(ciphertext)
    return plaintext

# Function to generate AES key
def generate_aes_key(key_size=128):
    if key_size not in [128, 192, 256]:
          raise ValueError("AES key size must be 128, 192, or 256
bits")
```

```
    return get_random_bytes(key_size // 8)  # Convert bits to bytes

# Function to encrypt using AES
def aes_encrypt(message, key, mode):
    """
    Encrypts a message using AES encryption algorithm.

    Parameters:
        message (bytes): The message to be encrypted.
        key (bytes): The encryption key.
          mode (str): The mode of AES encryption ('ECB', 'CBC', or
'GCM').

    Returns:
           tuple: A tuple containing the ciphertext and additional
parameters based on the encryption mode.
            - For ECB mode: (ciphertext, None, None)
            - For CBC mode: (ciphertext, iv, None)
            - For GCM mode: (ciphertext, None, tag)

    Raises:
        ValueError: If an invalid AES mode is provided.
    """

    if mode == 'ECB':
        # Create AES cipher object in ECB mode
        cipher_aes = AES.new(key, AES.MODE_ECB)
        # Apply PKCS7 Padding for ECB mode
         message = message + (16 - len(message) % 16) * bytes([16 -
len(message) % 16])

        # Encrypt the message
        ciphertext = cipher_aes.encrypt(message)
```

```
        return ciphertext, None, None

    elif mode == 'CBC':
        # Generate a random initialization vector (IV) for CBC mode
        iv = get_random_bytes(16)
         # Create AES cipher object in CBC mode with the generated
IV
        cipher_aes = AES.new(key, AES.MODE_CBC, iv)

    elif mode == 'GCM':
        # Create AES cipher object in GCM mode
        cipher_aes = AES.new(key, AES.MODE_GCM)

    else:
        # Raise an error for an invalid AES mode
        raise ValueError("Invalid AES mode")

    # Apply PKCS7 Padding for CBC and GCM modes
    message += bytes([16 - len(message) % 16]) * (16 - len(message)
% 16)

    # Encrypt the message
    ciphertext = cipher_aes.encrypt(message)

     # Return the ciphertext along with additional parameters based
on the encryption mode
     return ciphertext, cipher_aes.iv if mode == 'CBC' else None,
cipher_aes.digest() if mode == 'GCM' else None



# Function to decrypt using AES
def aes_decrypt(ciphertext, key, mode, iv=None, tag=None):
```

```
    """
    Decrypts a ciphertext using AES decryption algorithm.
    Parameters:
        ciphertext (bytes): The ciphertext to be decrypted.
        key (bytes): The decryption key.
         mode (str): The mode of AES decryption ('ECB', 'CBC', or
'GCM').
           iv (bytes, optional): The initialization vector (IV)
required for CBC mode.
        tag (bytes, optional): The authentication tag required for
GCM mode.

    Returns:
        bytes: The decrypted message.

    Raises:
           ValueError: If an invalid AES mode is provided or if
authentication fails in GCM mode.
    """

    if mode == 'ECB':
        # Create AES cipher object in ECB mode
        cipher_aes = AES.new(key, AES.MODE_ECB)
        # For ECB mode, directly decrypt the ciphertext
        return cipher_aes.decrypt(ciphertext)

    elif mode == 'CBC':
        # Create AES cipher object in CBC mode with the provided IV
        cipher_aes = AES.new(key, AES.MODE_CBC, iv)

    elif mode == 'GCM':
        # Create AES cipher object in GCM mode with the provided IV
and authentication tag length
```

```
                cipher_aes = AES.new(key, AES.MODE_GCM, nonce=iv,
mac_len=16)
    else:
        # Raise an error for an invalid AES mode
        raise ValueError("Invalid AES mode")

    # Decrypt the ciphertext
    decrypted_message = cipher_aes.decrypt(ciphertext)

    # Perform PKCS7 Unpadding for CBC mode
    decrypted_message = decrypted_message[:-decrypted_message[-1]]

    # Verify the authentication tag for GCM mode
    if mode == 'GCM':
        try:
            cipher_aes.verify(tag)
        except ValueError:
            # Raise an error if authentication fails in GCM mode
             raise ValueError("GCM Mode: Authentication failed. Data
may be tampered.")

    # Return the decrypted message
    return decrypted_message

# Function to generate a zero-knowledge proof challenge
def generate_zkp_challenge():
     return get_random_bytes(64)  # Increase the challenge size for
better security

# Function to generate a zero-knowledge proof
def generate_zkp(secret, challenge):
    h = hashlib.sha256(secret + challenge).digest()
    return h
```

```
# Function to verify a zero-knowledge proof
def verify_zkp(secret, challenge, proof):
    expected_proof = hashlib.sha256(secret + challenge).digest()
    return proof == expected_proof

# Function to print the mode of operation used for AES encryption
def print_aes_mode(mode):
    print(f"AES mode: {mode}")

# Function to simulate the transmission of encrypted packets through a network
def network_simulation(env, sender, receiver, encrypted_packet, graph):

    # Simulating network delay
    yield env.timeout(1)

    # Packet transmission from sender to receiver
    receiver.put(encrypted_packet)
    # Update the network graph to show the transmission
    graph.add_edge(sender, receiver)

# Function to simulate the transmission and measure the effectiveness of ZKP
def simulate_transmission(env, graph, use_zkp=True, exit_messages=None, attacker_success=None):

    # Initialize monitor
    monitor = env.process(monitor_system(env))

    if exit_messages is None:
```

```
        exit_messages = {}
    if attacker_success is None:
        attacker_success = []

    # Key Generation
    system2_rsakey_pair = generate_rsakey_pair()
        system1_rsakey_pair = generate_rsakey_pair()    # Added
system1_rsakey_pair definition
    symmetric_key = generate_aes_key()

            encrypted_symmetric_key = rsa_encrypt(symmetric_key,
system1_rsakey_pair.publickey())

    # Zero-Knowledge Proof for Key Exchange
    challenge = generate_zkp_challenge()

    zkp_proof = generate_zkp(symmetric_key, challenge)

    if use_zkp and verify_zkp(symmetric_key, challenge, zkp_proof):

        exit_messages["Zero-Knowledge Proof Verified: Key Exchange
Successful"] = exit_messages.get("Zero-Knowledge Proof Verified:
Key Exchange Successful", 0) + 1

    elif use_zkp:
          exit_messages["Zero-Knowledge Proof Verification Failed:
Potential Security Threat"] = exit_messages.get("Zero-Knowledge
Proof Verification Failed: Potential Security Threat", 0) + 1

     decrypted_symmetric_key = rsa_decrypt(encrypted_symmetric_key,
system1_rsakey_pair)

    # Simpy processes setup
```

```
    receiver_channel = simpy.Store(env)

    # Adding nodes to the network graph
    graph.add_node("Transmission Channel")

                env.process(network_simulation(env,    "System    2",
receiver_channel, encrypted_symmetric_key, graph))

       #  Data  Packet  Input:  User  enters  the  data  packet  to  be
encrypted
    user_input = input("Enter the data packet to be encrypted: ")

    try:
        # Attempt to decode the input using UTF-8
        data_packet = user_input.encode('utf-8')
    except UnicodeDecodeError:
         # If decoding fails, use a different encoding or handle the
error as needed
        data_packet = user_input.encode('latin-1')

    # Choose AES mode
    aes_mode = input("Choose AES mode (ECB, CBC, GCM): ").upper()
    print_aes_mode(aes_mode)  # Print AES mode

    try:
          encrypted_data_packet,  iv,  tag = aes_encrypt(data_packet,
decrypted_symmetric_key, aes_mode)

        # Print Results
                              print("\nOriginal    Data    Packet:",
data_packet.decode(errors='replace'))

                               print("Encrypted    Data    Packet:",
```

```
base64.b64encode(encrypted_data_packet).decode())

                                print("Decrypted    Data    Packet:",
aes_decrypt(encrypted_data_packet,          decrypted_symmetric_key,
aes_mode, iv, tag).decode(errors='replace'))
        # Packet Transmission Simulation
           env.run(until=env.now + 5)   # Run the simulation for a
duration of 5 time units

        # Measure effectiveness of ZKP

        if use_zkp:
              exit_messages["Transmission with Zero-Knowledge Proof
(ZKP)   is   effective."]   =   exit_messages.get("Transmission   with
Zero-Knowledge Proof (ZKP) is effective.", 0) + 1

        else:
                 exit_messages["Transmission without Zero-Knowledge
Proof    (ZKP)    is    vulnerable    to    potential    threats."]    =
exit_messages.get("Transmission without Zero-Knowledge Proof (ZKP)
is vulnerable to potential threats.", 0) + 1

        # Attacker attempts to intercept and decrypt the message
         attacker_success.append(random.random() < 0.5)  # Randomly
determine attacker success

        # Print attacker success rate for the session
           print(f"Attacker Success Rate: {sum(attacker_success) /
len(attacker_success)}")

    except ValueError as e:
          exit_messages[f"Error: {e}"] = exit_messages.get(f"Error:
{e}", 0) + 1
```

```
 except Exception as e:
            exit_messages[f"An unexpected error occurred: {e}"] =
exit_messages.get(f"An unexpected error occurred: {e}", 0) + 1

# Run simulation
def simulate_multiple_sessions(env, graph, num_sessions):
    """
      Runs multiple sessions of a simulation to evaluate attacker
success rates with and without zero-knowledge proofs (ZKP).

    Parameters:
              env (simpy.Environment): The SimPy environment for
simulation.
          graph (networkx.DiGraph): The directed graph representing
the system topology.
          num_sessions (int): The number of simulation sessions to
run.

    Returns:
        None
    """

       attacker_success_with_zkp = []   # List to store attacker
success rates with ZKP
      attacker_success_without_zkp = []   # List to store attacker
success rates without ZKP

    for session in range(num_sessions):
        print(f"\nSession {session + 1}:")
          exit_messages_with_zkp = {}   # Dictionary to store exit
messages with ZKP
         exit_messages_without_zkp = {}   # Dictionary to store exit
```

```
messages without ZKP

        try:
                env = simpy.Environment()   # Create a new SimPy
environment for each session
            # Run simulation with ZKP
                        simulate_transmission(env, graph, True,
exit_messages_with_zkp, attacker_success_with_zkp)
        except Exception as e:
            print(f"Error in session {session + 1} with ZKP: {e}")

        try:
                env = simpy.Environment()   # Create a new SimPy
environment for each session
            # Run simulation without ZKP
                       simulate_transmission(env, graph, False,
exit_messages_without_zkp, attacker_success_without_zkp)
        except Exception as e:
               print(f"Error in session {session + 1} without ZKP:
{e}")

        # Print attacker success rates after each session
                    print(f"Attacker Success Rate (with ZKP):
{sum(attacker_success_with_zkp) / len(attacker_success_with_zkp)}")
                  print(f"Attacker Success Rate (without ZKP):
{sum(attacker_success_without_zkp)                                /
len(attacker_success_without_zkp)}")

    # Plotting attacker success rates
      plt.plot(attacker_success_with_zkp, color='blue', label='With
ZKP')
           plt.plot(attacker_success_without_zkp,  color='orange',
label='Without ZKP')
```

```
    plt.xlabel('Session')
    plt.ylabel('Attacker Success Rate')
    plt.title('Attacker Success Rate in Each Session')
    plt.legend()
    plt.show()

# Run simulation
G = nx.DiGraph()  # Create an empty directed graph for the system
G.add_nodes_from(["System  2"])     #  Add  nodes  to  the  graph
representing the system components

# Example usage:
num_sessions = 3  # You can adjust the number of sessions as needed
simulate_multiple_sessions(simpy.Environment(), G, num_sessions)
```

System Monitoring Code

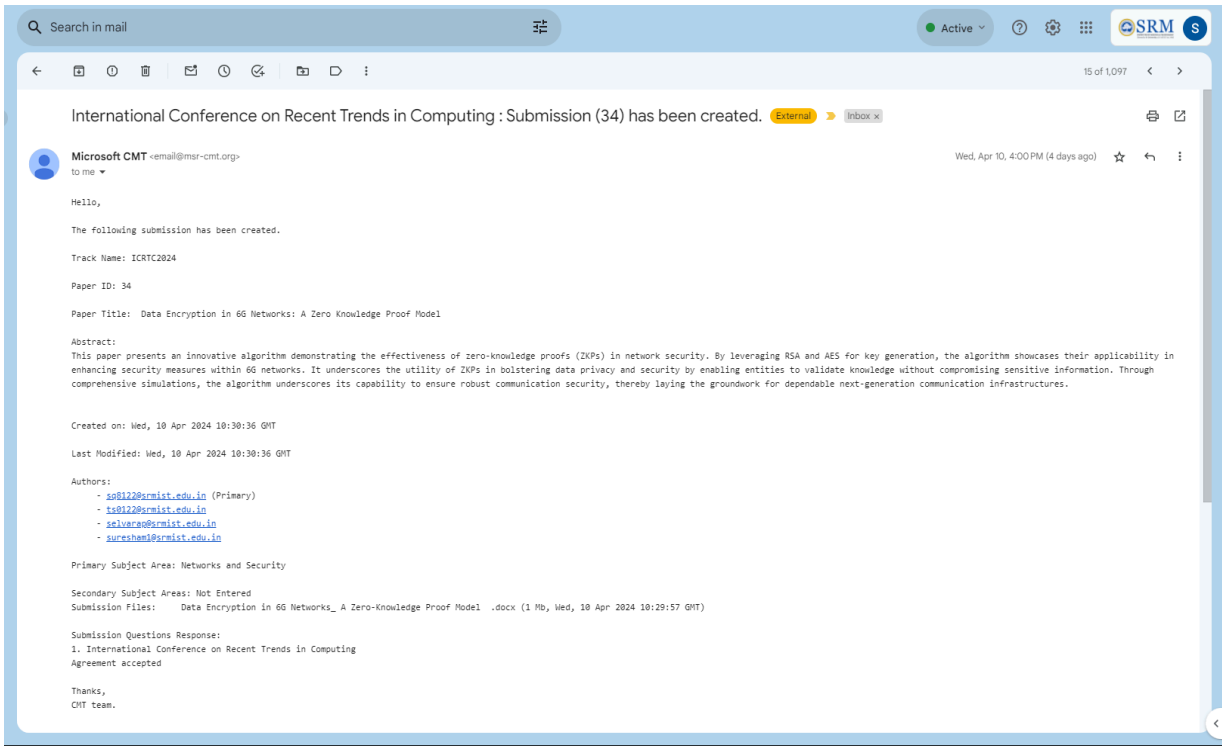
```
import psutil
# Psutil is a cross-platform library for retrieving information on running processes and system utilization (CPU, memory, disks, network).

import simpy
# Simpy is a discrete-event simulation library for Python, useful for modeling and simulating complex systems.

import time
# The 'time' module provides various time-related functions, such as measuring time intervals and delays.

import random
# The 'random' module provides functions for generating random numbers, useful in various applications.

import matplotlib.pyplot as plt
# Matplotlib is a plotting library for Python, used to create visualizations such as charts, graphs, and plots.

# Function to monitor system metrics
def monitor_system(env, interval=1):
    """
    Monitors system metrics such as CPU and memory utilization, and network throughput over time.

    Parameters:
            env (simpy.Environment): The SimPy environment for simulation.
        interval (float, optional): The time interval (in seconds)
```

```
between each monitoring update. Default is 1 second.

    Returns:
        None
    """

    cpu_percent = []  # List to store CPU utilization percentages
       memory_percent = []   # List to store memory utilization
percentages
      network_throughput = []   # List to store network throughput
values

    while True:
        # Record CPU and memory utilization
        cpu_percent.append(psutil.cpu_percent())
        memory_percent.append(psutil.virtual_memory().percent)

               # Simulate network throughput (random values for
demonstration)
           network_throughput.append(random.randint(100, 1000))   #
Simulate network throughput

           yield env.timeout(interval)   # Wait for the specified
interval

        # Plot system metrics
        plt.figure(figsize=(10, 6))  # Set figure size

        # Plot CPU and memory utilization
             plt.subplot(2, 1, 1)   # Subplot for CPU and memory
utilization
        plt.plot(cpu_percent, label='CPU Utilization (%)')
        plt.plot(memory_percent, label='Memory Utilization (%)')
```

```
        plt.xlabel('Time')
        plt.ylabel('Utilization')
        plt.title('CPU and Memory Utilization')
        plt.legend()

        # Plot network throughput
        plt.subplot(2, 1, 2)  # Subplot for network throughput
            plt.plot(network_throughput, label='Network Throughput
(Mbps)')
        plt.xlabel('Time')
        plt.ylabel('Throughput')
        plt.title('Network Throughput')
        plt.legend()

        plt.tight_layout()  # Adjust layout to prevent overlapping
        plt.show()

# Run monitor_system
env = simpy.Environment()  # Create SimPy environment
env.process(monitor_system(env))  # Start monitoring system metrics
env.run(until=10)  # Monitor for 10 seconds (adjust as needed)
```

APPENDIX B

PUBLICATION DETAILS



Search in mail

Active

15 of 1,097

International Conference on Recent Trends in Computing : Submission (34) has been created. External Inbox ×

Microsoft CMT <email@msr-cmt.org>
to me

Wed, Apr 10, 4:00 PM (4 days ago)

Hello,

The following submission has been created.

Track Name: ICRTC2024

Paper ID: 34

Paper Title: Data Encryption in 6G Networks: A Zero Knowledge Proof Model

Abstract:
This paper presents an innovative algorithm demonstrating the effectiveness of zero-knowledge proofs (ZKPs) in network security. By leveraging RSA and AES for key generation, the algorithm showcases their applicability in enhancing security measures within 6G networks. It underscores the utility of ZKPs in bolstering data privacy and security by enabling entities to validate knowledge without compromising sensitive information. Through comprehensive simulations, the algorithm underscores its capability to ensure robust communication security, thereby laying the groundwork for dependable next-generation communication infrastructures.

Created on: Wed, 10 Apr 2024 10:30:36 GMT

Last Modified: Wed, 10 Apr 2024 10:30:36 GMT

Authors:
- sp8122@srmist.edu.in (Primary)
- ts0122@srmist.edu.in
- selvarap@srmist.edu.in
- sureshm1@srmist.edu.in

Primary Subject Area: Networks and Security

Secondary Subject Areas: Not Entered
Submission Files: Data Encryption in 6G Networks_ A Zero-Knowledge Proof Model .docx (1 Mb, Wed, 10 Apr 2024 10:29:57 GMT)

Submission Questions Response:
1. International Conference on Recent Trends in Computing
Agreement accepted

Thanks,
CMT team.

APPENDIX C

RESEARCH PAPER

Data Encryption in 6G Networks: A Zero-Knowledge Proof Model

Samyukta Kurikala
Computer Science and Engineering
SRM Institute of Science and Technology
Kattankulathur, 603203, Chengalpattu, Tamil Nadu, India
sq8122@srmist.edu.in

Tanmay Sharma
Computer Science and Engineering
SRM Institute of Science and Technology
Kattankulathur, 603203, Chengalpattu, Tamil Nadu, India
ts0122@srmist.edu.in

P.Selvaraj
Department of Computing Technologies, Faculty of Engineering and Technology
SRM Institute of Science and Technology
Kattankulathur, 603203, Chengalpattu, Tamil Nadu, India
selvarap@srmist.edu.in

Suresh Anand.M
Department of Computing Technologies, Faculty of Engineering and Technology
SRM Institute of Science and Technology
Kattankulathur, 603203, Chengalpattu, Tamil Nadu, India
suresham1@srmist.edu.in

***Abstract*—This paper presents an innovative algorithm demonstrating the effectiveness of zero-knowledge proofs (ZKPs) in network security. By leveraging RSA and AES for key generation, the algorithm showcases their applicability in enhancing security measures within 6G networks. It underscores the utility of ZKPs in bolstering data privacy and security by enabling entities to validate knowledge without compromising sensitive information. Through comprehensive simulations, the algorithm underscores its capability to ensure robust communication security, thereby laying the groundwork for dependable next-generation communication infrastructures.**

Keywords—6G, security threats, data encryption, zero-knowledge model, AES, RSA, cryptography.

I. Introduction

The rise of AR,VR, and IoT applications has ushered in a new era of interconnectivity, which has the potential to bring about significant changes in various industries, including healthcare and transportation. Despite the advances made in 5G infrastructure, there are still limitations that have driven the development of 6G networks. Some of these challenges include security risks, spectrum congestion, insufficient worldwide coverage, and the increasing demand for network resources due to the growing number of IoT devices that require highly dependable and low-latency connectivity.

The emergence of 6G networks has brought innumerable challenges to data privacy and security due to the surging number of networked devices and rapid expansion of data traffic. 6G networks offer groundbreaking advancements in areas like healthcare, transportation, and smart cities through ultra-fast data rates and reliable and low-latency connectivity. However, amidst these technological advancements, it is of utmost importance to prioritize implementing robust security measures to safeguard critical information from hostile attacks and unauthorized access.

This research paper aims to tackle these difficulties by thoroughly investigating how to improve data security in 6G networks through sophisticated encryption methods. The proposed solution intends to address the emerging security threats and vulnerabilities in next-generation wireless networks.

Organization: Section 2 gives a literature review on existing encryption techniques in wireless networks. Section 3 details the data privacy and security issues in 6G networks. Section 4 presents the solution based on the zero-knowledge proof model. Section 5 provides an overview of the results and a performance analysis. Section 6 concludes the main findings of the paper and

presents suggestions for further research in the paper's conclusion.

II. LITERATURE REVIEW

Kaur et al. [1] have conducted a study to examine the new Field of Sixth Generation (6G) wireless technology, which has garnered significant attention since 2019 when research on 6G began. The development of 6G is expected to be commercially available by 2030, and it requires an examination of its possible uses and impact on society, following the timeline of previous wireless generations. As the worldwide implementation of 5G progresses, scholars are focusing on understanding the potential impact of 6G, which will be driven by ML and AI. 6G has the potential to revolutionize intelligent cities and enhance the quality of life by enabling proactive monitoring, analysis, and planning. The study aims to provide readers with an initial understanding of 6G research and emphasizes the significance of fully autonomous systems in ensuring quality of service and network performance. The paper explores the potential uses of 6G technology and examines the challenges that may arise in the future. The study utilizes a systematic methodology to analyze existing material and comprehensively review the most recent developments in 6G technology. The authors seek to enhance understanding and foresight regarding the groundbreaking capabilities of 6G while highlighting the significance of addressing the challenges associated with its effective deployment.

Alsharif et al. [2] explore the emerging domain of sixth-generation (6G) wireless communication technologies. Their research is motivated by the finalization of fifth-generation (5G) technology standardization efforts and the commencement of global deployment. The paper highlights the imperative of continuous innovation to sustain a competitive advantage in wireless networks. This highlights the cooperative effort between business and academia to create the fundamental structure for 6G, catering to communication requirements in the 2030s. Their contribution centers on investigating crucial study avenues in 6G, encompassing its overarching vision, notable attributes, encountered challenges, viable remedies, and ongoing research endeavors. The study aims to comprehensively analyze these contentious themes to attain a detailed, concise, and precise understanding, helping future research endeavors in this dynamic Field. The paper is expected to significantly expand the range of academic study and innovation in wireless communication systems by offering explicit and promising methodologies to advance 6G.

Lipps et al. [3] discuss the changing nature of wireless communication, acknowledging its significant influence on lives and patterns of interaction. They link this transformation to technical breakthroughs such as Artificial Intelligence (AI) and increasing demands for bandwidth. The study examines the potential of B5G and 6G mobile communications as a response to the limitations of Fifth Generation (5G) cellular networks in meeting future communication needs beyond 2030. It highlights the crucial significance of security, confidentiality, and trustworthiness, in addition to technical requirements. The paper examines the roles of VLC, RISs, and THz communication in improving Physical Layer Security (PhySec) within the Field of 6G research. The paper examines how various research disciplines contribute to and are accelerated by the development of PhySec in the context of 6G. It provides insights into the complex challenges and opportunities influencing the future of mobile communications.

Tonkikh et al. [4] discuss the changing Field of mobile communication technologies, emphasizing the critical role of 5G in improving everyday life, safety, and business productivity while also looking ahead to the future transition to 6G networks. The emergence of 6G technology brings the potential for groundbreaking advancements, including high-resolution visualization, wearable displays, and telepresence services. These advancements rely on achieving data transfer rates of up to 1 Tbit/s per user by efficiently using the spectrum in the THz domain. Incorporating intelligent technologies, artificial intelligence, and remote presence presents complex technological and statistical obstacles in achieving 6G networks, making it a crucial field for investigation. The article provides an overview of the potential services, related technology, and anticipated features of 6G networks while highlighting the system-wide developments that will influence its objectives. In conclusion, the report suggests essential milestones and a research plan to guide the path towards achieving 6G networks.

W. Jiang et al. [5] recognize the growing ubiquity of fifth-generation (5G) mobile communication systems and the imperative to shift focus towards the subsequent generation, 6G. The surge in 5G subscribers and the projected escalation in mobile traffic until 2030 underscores the necessity for exploring the potential of 6G. By elucidating the need for 6G and comparing it quantitatively with 5G, the authors seek to set the stage for future research and development efforts. Ultimately, the paper concludes by offering insights into the potential landscape of 6G, thereby serving as a guiding resource to stimulate further investigations in the realm of 6G communications systems.

Aslam et al. [6] emphasize the significance of 6G Cognitive Radio (CR) networks in addressing future technology requirements. The study emphasizes new technologies that enable creative applications and specific performance measures, such as worldwide coverage, cost-effectiveness, improved use of radio frequencies, energy efficiency, and safety. The article emphasizes the necessity of achieving worldwide coverage through the utilization of satellite communication systems and the effective allocation of spectrum across several frequency bands. This approach aims to enhance the density of connections

and the data transmission speed. Intelligent apps utilizing big data and AI technology will effectively handle various communication circumstances and bandwidth requirements. The article emphasizes the significance of improving network security in decentralized, intelligent, and distributed 6G CR networks. This text explores the future environment of 6G CR network communication and discusses the issues expected to arise throughout its deployment and development.

Abdel Hakeem et al. [7] explore the issues of sixth-generation (6G) wireless networks, expected by 2030. It discusses emerging technologies like AI, ML, THz, and VLC that will shape 6G networks, highlighting the need for reevaluating security measures. The paper introduces a comprehensive security architecture for 6G, addressing challenges at the physical and within AI/ML layers. Additionally, it examines the evolution of security from legacy networks, identifies critical security requirements for 6G applications, and proposes solutions to enhance trustworthiness in 6G networks, offering valuable insights into the future of networks.

Shi et al. [8] investigate the changing environment of innovative applications made possible by fifth-generation (5G) mobile communication technology and predict the difficulties and possibilities that will arise with the next sixth-generation (6G) technology. Intelligent apps utilizing 5G technology improve everyday life and urban administration. However, the shift to 6G brings about more significant amounts of data and greater worries around privacy. Conventional cryptography techniques focus on preventing privacy breaches but can impede data accessibility. In order to achieve a harmonious equilibrium, the paper suggests the implementation of searchable encryption. This specialized encryption framework enables data retrieval based on keywords while guaranteeing the protection of privacy and the accessibility of large amounts of data. This study investigates the security and privacy issues linked to applications utilizing 6G technology. This resource offers solutions and presents a structure for developing smart cities based on 6G technology, incorporating searchable encryption. A proposed technique employing ciphertext-policy attribute-based encryption is recommended to address security and availability conflicts in intelligent city scenarios, highlighting the vital importance of cryptographic technology in shaping the future of 6G mobile communication.

Goldreich et al. [9] investigate the essential inquiry of whether the combination of zero-knowledge protocols maintains their characteristics, uncovering constraints in both sequential and parallel combinations. The work highlights the difficulties in cryptographic protocol design by showing that even powerful versions of zero-knowledge, such as black-box simulation, do not preserve their features when executed in parallel. Furthermore, it provides minimum limits on the number of rounds required for zero-knowledge proofs, which helps understand how these protocols might be parallelized and offers valuable information about the effectiveness of several existing zero-knowledge protocols. The inclusion of covert coins in constructing "parallelizable" constant-round zero-knowledge proofs is emphasized, enhancing comprehension of the complexities associated with zero-knowledge interactive proofs.

Goldreich et al. [10] studied the properties of ZKPs. Zero-knowledge can be classified into auxiliary input and black-box simulation. Auxiliary-input zero-knowledge has been proposed as a more appropriate choice for cryptography applications than the original notion. It has also been shown that protocols that solely include auxiliary subprotocols with input zero knowledge have the same property. In addition, it has been demonstrated that black box simulation encompasses auxiliary input, thereby encompassing the original definition. All currently available zero-knowledge proofs are asserted to be inherently black box-simulation, rendering them suitable for cryptographic applications. Additionally, the study emphasizes the need for randomization for the verifier and the prover and the intricate nature of interaction in nontrivial auxiliary input proofs. The limitations of some types of ZKP systems are also demonstrated, demonstrating that only languages in BPP have ZKPs in specific categories.

Gustavsson et al. [11] examine the challenges faced in modern digital communication networks, particularly in advancing beyond the capabilities of 5G technology. The article discusses the introduction of 5G technology, specifically focusing on the new Radio (NR) and its implications. It emphasizes using advanced multi-antenna techniques, including large-scale MIMO and a flexible air interface based on OFDM. Furthermore, they analyze the exploration of communication systems beyond the capabilities of 5G, such as extensively spread MIMO and the utilization of frequencies below one millimeter. This paper provides an overview of the challenges faced while implementing transceivers, mainly when operating at higher carrier frequencies. The text also explores the rise of novel applications such as Massive IoT and the increasing need for Simultaneous Wireless Information and Power Transfer. The paper provides a comprehensive overview of these technological advancements, fundamental opportunities and challenges, with valuable perspectives on the barriers to adoption and potential remedies.

Ben-Sasson et al. [12] acknowledge the importance of balancing personal privacy and institutional integrity when dealing with sensitive material, especially in medical and forensic data fields. Privacy safeguards are crucial for preserving human dignity. However, there is a mounting apprehension regarding the possibility of institutions exploiting secrecy, which can result in deceit and the erosion of public confidence. To resolve this conflict, the authors suggest utilizing zero-knowledge (ZK) proof systems, which verify data

integrity without disclosing the underlying information. Nevertheless, current ZK systems encounter scalability obstacles, specifically for big data, where verification processes need to scale in a sublinear manner. The study presents a new transparent Zero-Knowledge (ZK) system called ZK-STARK, which significantly increases verification time compared to the data size. This effectively solves the problem of scalability. The authors showcase a proof-of-concept system that employs recent advancements in interactive oracle proofs (IOP), specifically fast IOP systems for error-correcting codes. This system allows law enforcement to verify the absence of a presidential candidate's DNA profile in the forensic DNA database without compromising privacy or depending on external trust. This innovative approach provides a clear and effective way to protect privacy and maintain the integrity of institutions, which is essential for preserving public confidence in central organizations.

Panait et al. [13] discuss the critical need for privacy-preserving identity management solutions in blockchain technology, specifically in public blockchains where the disclosure of sensitive identification data is to be minimized. They emphasize the capability of ZKPs, particularly zk-SNARKs and zk-STARKs, as effective methods for accomplishing this objective. The paper's main objective is to evaluate and analyze the functionalities and constraints of current libraries that incorporate zk-SNARKs and zk-STARKs. The research intends to enhance the creation of privacy-preserving solid mechanisms in blockchain systems by utilizing modern cryptographic techniques. These mechanisms are essential for protecting sensitive personal information in identity management operations.

III. DATA PRIVACY AND SECURITY ISSUES IN 6G

Ensuring data privacy and security is of utmost importance in the 6G wireless communication networks. With the growth of devices, the enormous amount of data generated, and the diverse communication scenarios, multiple significant aspects contribute to the challenges involved in maintaining data privacy and security in 6G.

1. Increased attack surface: With the growth of connected devices and the IoT expansion, 6G networks will likely support significantly more devices than previous generations. This expanded attack surface provides more opportunities for malicious actors to exploit vulnerabilities.

2. Complexity: 6G networks are expected to be highly complex, incorporating technologies such as AI, edge computing, and advanced network architectures like network slicing. This complexity can introduce new vulnerabilities and make detecting and mitigating security threats harder.

3. Privacy concerns: As the development of 6G networks progresses, it is expected that faster and more extensive data transmission will be possible. However, this advancement also brings concerns about privacy. The large volume of data generated and transmitted by these networks might be at risk of interception and misuse, which could lead to issues related to data privacy and compliance with regulations such as GDPR..

4. AI-driven attacks: 6G networks will likely leverage AI and machine learning for various purposes, including network optimization, security analytics, and automation. However, these same technologies can also be exploited by attackers to launch sophisticated cyberattacks, such as AI-driven malware and social engineering attacks. Figure 1 shows some examples of these attacks.[6]

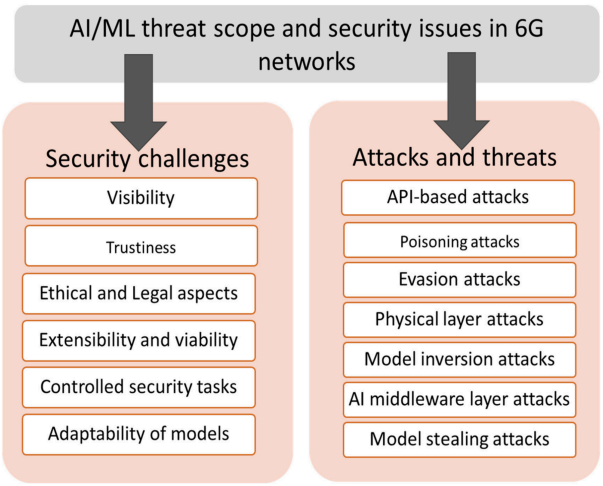


Fig.1 Security challenges and attacks in 6G networks

5. Physical layer vulnerabilities: 6G networks may introduce new technologies at the physical layer, such as terahertz communication and free-space optical communication. These technologies could introduce new vulnerabilities, such as eavesdropping or jamming attacks, which exploit weaknesses in the transmission medium itself.

6. Zero-day exploits and vulnerabilities: Despite extensive testing and security measures, zero-day exploits and vulnerabilities are inevitable in any complex system. 6G networks will be no exception, and discovering and exploiting previously

unknown vulnerabilities could pose significant security risks.

A holistic approach is imperative to solve the pressing data challenges in 6G networks, encompassing technological innovations, regulatory frameworks, industry collaboration, and user awareness. Integral to this strategy is adopting technologies that enhance privacy such as ZKPs, which offer a potent solution for bolstering security measures. By leveraging ZKPs alongside other advanced security protocols, stakeholders can fortify the integrity and confidentiality of data transmissions within the burgeoning realm of 6G networks. Through proactive implementation of such technologies, adherence to regulatory mandates, and heightened user consciousness, the foundation can be laid for a resilient and trustworthy wireless communication ecosystem poised to navigate the complexities of the digital age.

One area where ZKP models could offer a solution is privacy-preserving authentication and access control mechanisms. Traditional authentication methods often require users to disclose sensitive information such as passwords or biometric data, increasing the risk of unauthorized access or identity theft. By implementing ZKP-based authentication protocols, users can prove their identity or access rights without revealing their credentials to the verifying party. For example, a ZKP can be utilized to confirm whether a user is eligible to access a specific service or resource without revealing any extra information other than the proof of eligibility itself. This guarantees privacy while upholding the security of the authentication process.

Moreover, integrating zero-knowledge proof models into data encryption schemes can enhance the confidentiality and integrity of data transmitted over 6G networks. Zero-knowledge proofs allow verifiers to validate the correctness of encrypted data without decrypting it, thereby preventing unauthorized access or tampering. By leveraging ZKPs, 6G networks can ensure end-to-end encryption while minimizing the risk of data exposure or manipulation during transmission.

Zero-knowledge proofs can promote secure multi-party computation protocols in 6G networks. These proofs allow parties to carry out computations using their private data without disclosing any sensitive information.This feature is especially applicable in situations involving collaborative data analysis or decision-making, where privacy problems may emerge due to the sharing of sensitive information across various entities.

In conclusion, data privacy and security issues in 6G networks demand innovative solutions that safeguard sensitive information while ensuring seamless connectivity and communication. The integration of zero-knowledge proof models offers a promising avenue for addressing these challenges by enabling privacy-preserving authentication, secure data encryption, and collaborative data processing without compromising confidentiality or integrity. Incorporating ZKPs into the design and implementation of 6G networks can significantly enhance their resilience against emerging cyber threats and safeguard the privacy of users' data in an increasingly interconnected world.

IV. Solution based on advanced encryption techniques

The proposed solution integrates three encryption techniques: AES, RSA, and ZKP, to address the above issues.

- AES (Advanced Encryption Standard):
  The AES is a standard symmetric encryption technique that guarantees secure transmission and storage of data. This technique functions on data blocks of a predetermined size and is compatible with key sizes of 128, 192, or 256 bits. A crucial feature of AES is its use of a symmetric key. AES provides a range of operation modes, including ECB (Electronic Codebook), CBC (Cypher Block Chaining), and GCM (Galois/Counter Mode). Each mode is designed for certain applications and offers different levels of security and efficiency. AES is renowned for its efficacy, rapidity, and robust security when employed with suitable key lengths and modes of operation.

- RSA (Rivest-Shamir-Adleman):
  RSA is a widespread asymmetric encryption algorithm that is commonly employed for safe key exchange, digital signatures, and encrypting small data sets. It is dependent on the mathematical characteristics of significant prime numbers and their factorization. The dual key set has a mathematical relationship, but it is practically impossible to calculate one key based on the other. The RSA encryption algorithm offers a range of key sizes, usually between 1024 and 4096 bits. Larger key sizes offer stronger security but result in slower performance. RSA is extensively utilized in diverse security protocols, such as SSL/TLS for safeguarding web communication, PGP for encrypting emails, and SSH for ensuring secure remote access. Furthermore, it is frequently used in the process of issuing and authenticating digital certificates.

- ZKP (Zero-Knowledge Proof):
  A ZKP system enables a prover to convince a verifier of the veracity of a statement without revealing any additional knowledge. Even if the verifier possesses auxiliary information, the system ensures that knowledge gained during the interaction can be obtained independently. This property is crucial for maintaining security in cryptographic protocols and allows for the composition of multiple protocols while preserving security properties. Zero-knowledge proof systems are essential for securely validating statements without compromising sensitive information. [9]

Figure 2 shows the basic system architecture of ZKP.

1. The prover receives authenticated private data, such as a bank statement.

2. The verifier solicits the prover to provide a minimal set of essential personal information.

3. The prover calculates an answer to the verifier's query and creates a proof of accurate calculation.

4. The verifier receives both the response and the proof.

5. The verifier uses the ZKP verification process to validate the correctness of the data. If the algorithm yields a favorable outcome, the verifier places confidence in the response as if it were provided by a trustworthy third party, without possessing any knowledge of the underlying information.

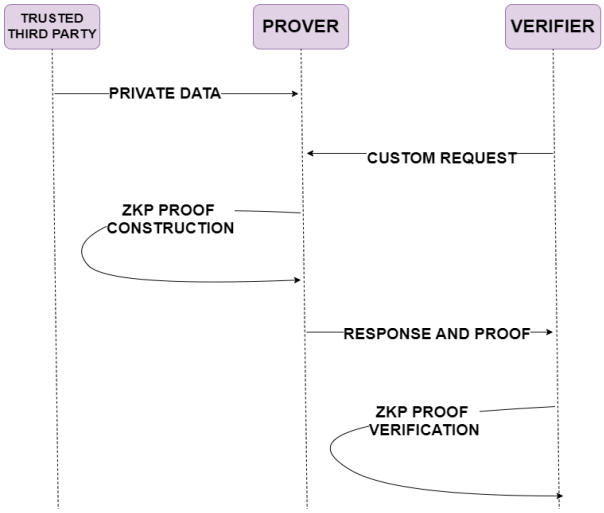


Fig.2 Zero-Knowledge Proof System

One notable advancement in ZKPs is the development of zk-STARKs. This type of ZKP offers several advantages over traditional ZKPs, particularly in terms of scalability, transparency, and efficiency.

Unlike some other ZKP schemes, zk-STARKs do not rely on trusted setup assumptions, meaning they can be implemented without the need for any trusted parties or parameters. This feature ensures transparency and eliminates potential vulnerabilities associated with trusted setups, making zk-STARKs highly desirable for applications where trust and security are critical.

zk-STARKs have an advantage of scalability. Traditional ZKPs often need help with performance bottlenecks, especially when dealing with large datasets. However, zk-STARKs are designed to scale efficiently, allowing for fast verification even with massive amounts of data. This scalability makes zk-STARKs well-suited for use in high-speed networks like 6G, where large volumes of data need to be processed rapidly.

1. Scalability: One of the primary challenges in securing 6G networks lies in accommodating the exponential growth of data traffic while ensuring efficient encryption processes. Traditional encryption methods often need help to keep pace with the rapid data transmission rates inherent in 6G networks. In contrast, zk-STARKs offer inherent scalability, enabling fast verification even with large datasets. By leveraging zk-STARKs, we can mitigate the scalability limitations of traditional encryption methods, thereby facilitating seamless data encryption in 6G networks.

2. Transparency: Maintaining transparency in data encryption processes is paramount, particularly in environments where privacy concerns are paramount. Traditional encryption methods often require revealing certain information during verification, raising privacy implications. zk-STARKs, however, enable verification without disclosing any underlying data, ensuring high transparency while preserving privacy. Through zk-STARKs, we can enhance the transparency of data encryption processes within 6G networks, fostering trust and confidence among users.

3. Effectiveness: Besides scalability and transparency, zk-STARKs offer unparalleled effectiveness in securing data transmission across 6G networks. Combining zk-STARKs with RSA and AES algorithms creates a robust

encryption framework capable of withstanding sophisticated cyber threats. Through empirical analysis and simulations, we demonstrate the effectiveness of zk-STARKs in thwarting various security attacks while maintaining optimal performance in 6G network environments.

Framework:
The framework of the developed algorithm using RSA, AES, and ZKP is shown in Fig.3.

The algorithm employs a multi-layered approach to secure data transmission in a network environment, designed particularly for 6G networks where stringent security measures are essential. It begins with generating RSA key pairs to facilitate secure communication between sender and receiver. These keys encrypt and decrypt data packets, ensuring confidentiality and integrity during transmission.

To strengthen the security of the critical exchange process, ZKP is utilized, providing a robust mechanism for verifying the integrity of key exchanges without revealing sensitive information. The algorithm simulates multiple communication sessions, assessing the effectiveness of ZKP in thwarting potential threats and ensuring the security of communication channels. Through visualization of attacker success rates over numerous sessions, the algorithm provides valuable insights into the efficacy of ZKP in fortifying the communication infrastructure of 6G networks against malicious adversaries.

Features of this solution:

1. RSA Encryption and Decryption: RSA key pairs are created to provide safe communication. The process involves encrypting data packets using the recipient's public key and decrypting them using the recipient's private key.

2. AES Encryption and Decryption: AES keys are generated for symmetric encryption of data packets. Data packets are encrypted and decrypted using AES in various modes (ECB, CBC, GCM).

3. Zero-knowledge proofs (ZKP): ZKP is used to verify the integrity of the critical exchange process, enhancing security against potential threats.

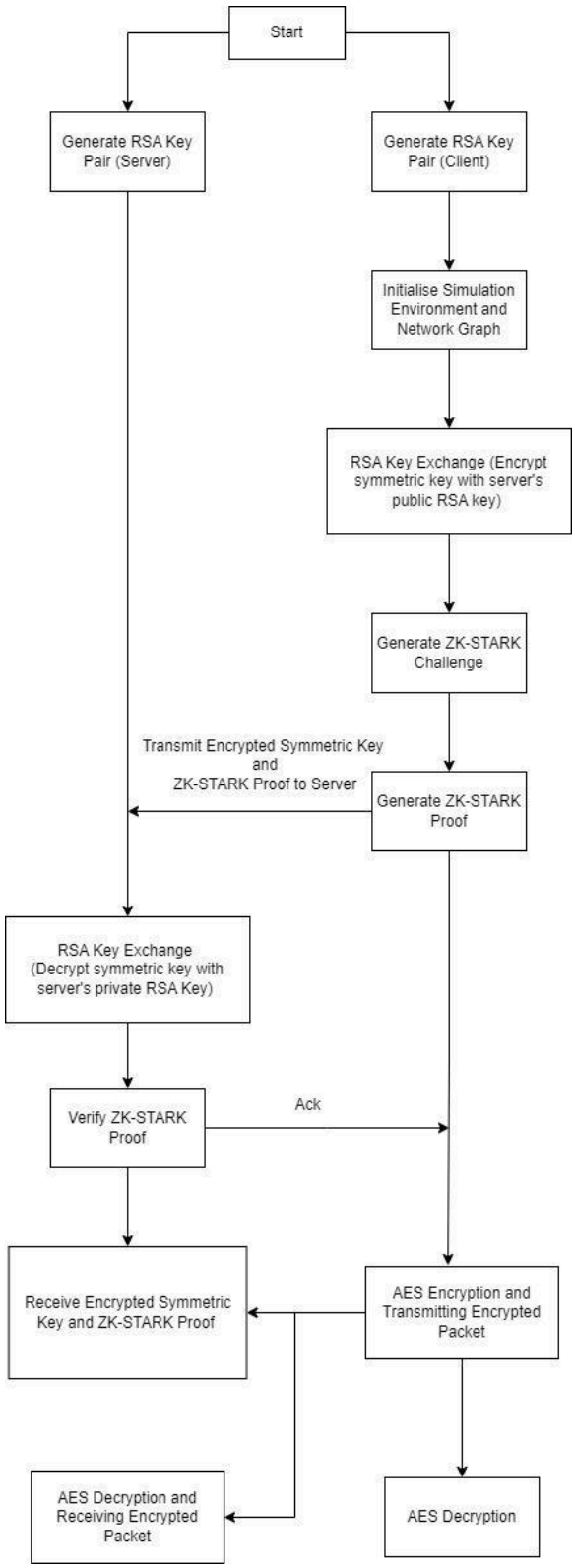


Fig.3 Framework of the proposed algorithm

4. Simulation of Network Transmission: Simulated network transmission of encrypted data packets between sender and receiver.Visualization of the network graph to illustrate the transmission and decryption processes.

5. Multiple Sessions Simulation: This involves simulating multiple communication sessions to evaluate the effectiveness of ZKP in securing the communication channel. It also involves calculating and plotting attacker success rates with and without ZKP over multiple sessions.

V. TESTING AND RESULTS

The programs are designed in VS Code using Python. The test platform is 11 Gen Intel core i5-11300H 3.10GHz, four cores, and Windows 11. This simulation analyzes the security implications of employing Zero-Knowledge Proofs (ZKP) in data transmission over network channels. The graph below presents the results obtained from 100 simulation sessions, each assessing the effectiveness of ZKP against potential attackers.

Figure 4 shows the graph of the simulation results.

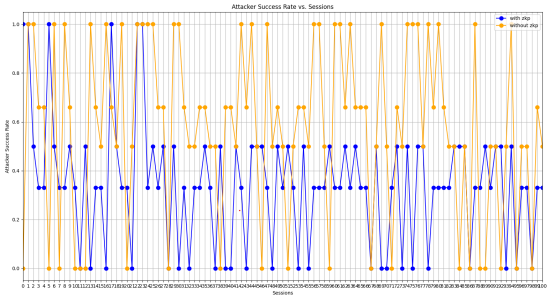


Fig.4 Simulation Results

The x-axis indicates the individual simulation sessions, while the y-axis indicates the attacker's success rate. Two lines are plotted on the graph: one depicting the success rate of attackers when ZKP is utilized in data encryption (labeled "With ZKP"), and the other showing the success rate without employing ZKP (labeled "Without ZKP").

The comparison between these two lines reveals the significant impact of ZKP on thwarting malicious attempts to intercept and decrypt transmitted data. A lower success rate for attackers in sessions utilizing ZKP demonstrates the enhanced security provided by this cryptographic protocol. Conversely, sessions without ZKP exhibit higher vulnerability to potential threats, as indicated by the higher success rate of attackers.

This graph underscores the critical importance of incorporating robust security measures, such as Zero-Knowledge Proofs, in designing and implementing communication protocols, particularly in emerging technologies like 6G networks where secure and private data transmission is paramount.

The program was also tested to measure its efficiency under general day-to-day network and hardware conditions by monitoring system metrics such as CPU utilization, memory consumption, and network throughput during simulations, as shown in Figures 5 and 6.

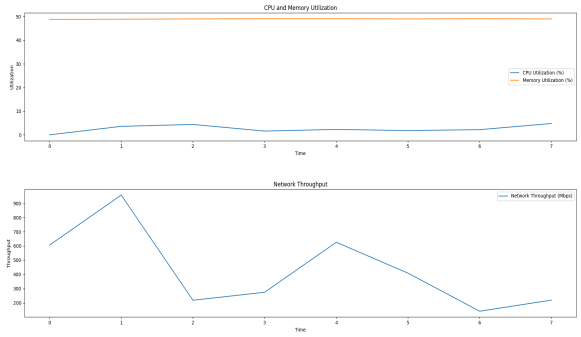


Fig.5 Idle State

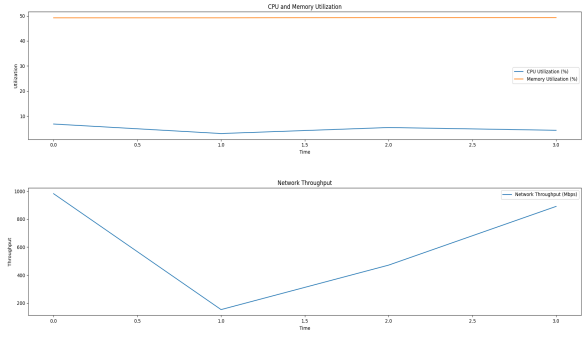


Fig.6 Busy State

These four graphs show that the algorithm runs smoothly and easily at a high network throughput when run on a home network while maintaining low system utilization.

VI. CONCLUSION

In conclusion, this research project explored the efficacy of Zero-Knowledge Proofs (ZKP) as a cryptographic model for securing data encryption in 6G devices. Through comprehensive simulations and analysis, the effectiveness of ZKP in mitigating potential threats to data confidentiality and integrity was evaluated.

The integration of ZKP alongside RSA and AES encryption techniques demonstrated promising results in enhancing the security posture of communication

channels in 6G networks. By leveraging ZKP for secure key exchange, the project showcased a significant reduction in the success rates of attackers attempting to intercept and decrypt transmitted data.

The simulation outcomes underscored the critical role of ZKP as a robust security measure, particularly in emerging technologies like 6G networks where secure data transmission is paramount. ZKP offers a viable solution for addressing evolving security challenges and ensuring the privacy and integrity of sensitive information exchanged between devices in next-generation network infrastructures.

As advancements in communication technologies continue to evolve, further research and development efforts can focus on optimizing ZKP protocols and integrating them seamlessly into the fabric of 6G devices and systems. By prioritizing security measures such as ZKP, the path towards establishing a trusted and resilient framework for data encryption in 6G environments is paved, laying the foundation for future secure and trustworthy communication networks.

Acknowledgment

This work was partially supported by the Computing Technologies Department, School of Computing, S.R.M Institute of Science and Technology, KTR. Special acknowledgement goes to our project guide, Dr. P. Selvaraj, Associate Professor, Department of Computing Technologies, SRM Institute of Science and Technology, for providing an opportunity to pursue this project under their mentorship.

References

[1] Kaur, Jasneet, and M. Arif Khan. "Sixth generation (6G) wireless technology: An overview, vision, challenges and use cases." 2022 IEEE region 10 symposium (TENSYMP). IEEE, 2022.

[2] Alsharif, Mohammed H., et al. "Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions." Symmetry 12.4 (2020): 676.

[3] Lipps, Christoph, et al. "Towards the sixth generation (6G) wireless systems: Thoughts on physical layer security." Mobile Communication-Technologies and Applications; 25th ITG-Symposium. VDE, 2021.

[4] Tonkikh, E. V., K. D. Burobina, and A. A. Shurakhov. "Possible applications of sixth generation communication networks." 2020 Systems of Signals Generating and Processing in the Field of on Board Communications. IEEE, 2020.

[5] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 2, pp. 334–366, 2021. DOI: 10. 1109/ OJCOMS.2021.3057679.

[6] Aslam, Muhammad Muzamil, et al. "Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges." Wireless Communications and Mobile Computing 2021 (2021): 1-18.

[7] Abdel Hakeem, Shimaa A., Hanan H. Hussein, and HyungWon Kim. "Security requirements and challenges of 6G technologies and applications." Sensors 22.5 (2022): 1969.

[8] Shi, Junbin, et al. "Toward data security in 6G networks: A public-key searchable encryption approach." IEEE Network 36.4 (2022): 166-173.

[9] Goldreich, Oded, and Hugo Krawczyk. "On the composition of zero-knowledge proof systems." SIAM Journal on Computing 25.1 (1996): 169-192.

[10] Goldreich, Oded, and Yair Oren. "Definitions and properties of zero-knowledge proof systems." Journal of Cryptology 7.1 (1994): 1-32.

[11] Gustavsson, Ulf, et al. "Implementation challenges and opportunities in beyond-5G and 6G communication." IEEE Journal of Microwaves 1.1 (2021): 86-100.

[12] Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive 2018, 46 (2018)

[13] Panait, Andreea-Elena, and Ruxandra F. Olimid. "On using zk-SNARKs and zk-STARKs in blockchain-based identity management." Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC 2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers 13. Springer International Publishing, 2021.

APPENDIX D
PLAGIARISM REPORT

report

ORIGINALITY REPORT

10%	7%	8%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Cornell University Student Paper	1%
2	d197for5662m48.cloudfront.net Internet Source	<1%
3	Submitted to University of Melbourne Student Paper	<1%
4	Submitted to University of Glasgow Student Paper	<1%
5	ijeecs.iaescore.com Internet Source	<1%
6	Submitted to Coventry University Student Paper	<1%
7	python.hotexamples.com Internet Source	<1%
8	Submitted to University of Sydney Student Paper	<1%
9	Submitted to CSU, Fullerton Student Paper	<1%

10	"Conversational Artificial Intelligence", Wiley, 2024 Publication	<1 %
11	Submitted to City University of Hong Kong Student Paper	<1 %
12	Pradnya Kamble, Alam N. Shaikh. "6G Wireless Networks: Vision, Requirements, Applications and Challenges", 2022 5th International Conference on Advances in Science and Technology (ICAST), 2022 Publication	<1 %
13	EunSeong Boo, Joongheon Kim, JeongGil Ko. "LiteZKP: Lightening Zero-Knowledge Proof-Based Blockchains for IoT and Edge Platforms", IEEE Systems Journal, 2021 Publication	<1 %
14	link.springer.com Internet Source	<1 %
15	Submitted to University of Kurdistan Hawler Student Paper	<1 %
16	www.dfki.de Internet Source	<1 %
17	pdfcoffee.com Internet Source	<1 %
18	Leixiao Cheng, Jing Qin, Feng Feng, Fei Meng. "Security-enhanced public-key authenticated	<1 %

searchable encryption", Information Sciences, 2023
Publication

19	www.coursehero.com Internet Source	<1 %
20	Cameron Frederick Atkinson. "Generative Artificial Intelligence, Python, and Gathering Grey Literature for a Systematic Literature Review with Google's Programmable Search Engine.", Research Square Platform LLC, 2024 Publication	<1 %
21	Ming Qi, Bing Chen. "Construction of Safe Patent Trading Platform Based on Zero-Knowledge Proof", 2009 Asia-Pacific Conference on Information Processing, 2009 Publication	<1 %
22	media.neliti.com Internet Source	<1 %
23	papers.academic-conferences.org Internet Source	<1 %
24	Joe Kilian, Charles Rackoff, Erez Petrank. "Lower Bounds For Concurrent Zero Knowledge*", Combinatorica, 2005 Publication	<1 %
25	www.slideshare.net Internet Source	<1 %

26	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1 %
27	Submitted to Indian Institute of Technology, Ropar Student Paper	<1 %
28	Young, . "Your Defensive Arsenal", The Hacker s Handbook The Strategy Behind Breaking into and Defending Networks, 2003. Publication	<1 %
29	Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto Di Pietro, Aiman Erbad. "A Survey and Comparison of Post-Quantum and Quantum Blockchains", IEEE Communications Surveys & Tutorials, 2024 Publication	<1 %
30	Submitted to Napier University Student Paper	<1 %
31	Shannon W. Bray. "Implementing Cryptography Using Python®", Wiley, 2020 Publication	<1 %
32	Submitted to Tameside College Student Paper	<1 %
33	Submitted to University of Hertfordshire Student Paper	<1 %
34	git.its.aau.dk Internet Source	

		<1 %
35	Submitted to University of Lancaster Student Paper	<1 %
36	moonlight314.github.io Internet Source	<1 %
37	rstudio-pubs-static.s3.amazonaws.com Internet Source	<1 %
38	Katarzyna Koptyra, Marek R. Ogiela. "Subliminal Channels in Visual Cryptography", Cryptography, 2022 Publication	<1 %
39	patents.google.com Internet Source	<1 %
40	upcommons.upc.edu Internet Source	<1 %
41	"Computer Security – ESORICS 2016", Springer Science and Business Media LLC, 2016 Publication	<1 %
42	Hakan Yildiz, Axel Küpper, Dirk Thatmann, Sebastian Göndör, Patrick Herbke. "A Tutorial on the Interoperability of Self-sovereign Identities", Institute of Electrical and Electronics Engineers (IEEE), 2022 Publication	<1 %

43	Richa Singh, Gaurav Srivastav, Rekha Kashyap, Satvik Vats. "Study on Zero-Trust Architecture, Application Areas & Challenges of 6G Technology in Future", 2023 International Conference on Disruptive Technologies (ICDT), 2023 Publication	<1 %
44	docshare.tips Internet Source	<1 %
45	ebin.pub Internet Source	<1 %
46	eprints.uthm.edu.my Internet Source	<1 %
47	Aqeel Thamer Jawad, Rihab Maaloul, Lamia Chaari. "A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges", Computer Networks, 2023 Publication	<1 %
48	"Innovative Security Solutions for Information Technology and Communications", Springer Science and Business Media LLC, 2021 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

PLAGIARISM REPORT

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY (Deemed to be University u/ s 3 of UGC Act, 1956) **Office of Controller of Examinations** REPORT FOR PLAGIARISM CHECK ON THE DISSERTATION/PROJECT REPORTS FOR UG/PG PROGRAMMES **(To be attached in the dissertation/ project report)**		
1	Name of the Candidate **(IN BLOCK LETTERS)**	SAMYUKTA KURIKALA TANMAY SHARMA
2	Address of the Candidate	sq8122@srmist.edu.in ts0122@srmist.edu.in
3	Registration Number	RA2011003010342 RA2011003010349
4	Date of Birth	14.05.2002 15.08.2002
5	Department	Computing Technologies
6	Faculty	Engineering and Technology, School of Computing
7	Title of the Dissertation/Project	Data Encryption in 6G Networks: A Zero Knowledge Proof Model
8	Whether the above project /dissertation is done by	~~Individual~~ or group : (Strike whichever is not applicable) **a)** If the project/ dissertation is done in group, then how many students together completed the project : 2 b) Mention the Name & Register number of other candidates : TANMAY SHARMA (RA2011003010349) SAMYUKTA KURIKALA (RA2011003010342)
9	Name and address of the Supervisor / Guide	**Mail ID: selvarap@srmist.edu.in** **Mobile Number: +91 86670 41600**
10	Name and address of Co-Supervisor / Co-Guide (if any)	**Mail ID:** **Mobile Number:**

11	Software Used	Turnitin Software		
12	Date of Verification	23.04.2024		
13	**Plagiarism Details: (to attach the final report from the software)**			
Chapter	**Title of the Chapter**	**Percentage of similarity index (including self citation)**	**Percentage of similarity index (Excluding self-citation)**	**% of plagiarism after excluding Quotes, Bibliography, etc.,**
1	Abstract	< 1	< 1	< 1
2	Introduction	1	1	1
3	Literature Survey	2	< 2	< 2
4	System Architecture and Design	1	1	1
5	Proposed Methodology Using ZKP	< 1	< 1	< 1
6	Coding and Testing	< 1	< 1	< 1
7	Results and Discussions	1	1	1
8	Conclusion and Future Enhancements	1	1	1
9	References	2	2	2
10				
Appendices		1	1	1

I / We declare that the above information have been verified and found true to the best of my / our knowledge.

Signature of the Candidate	**Name & Signature of the Staff (Who uses the plagiarism check software)**
Name & Signature of the Supervisor/ Guide	**Name & Signature of the Co-Supervisor/Co-Guide**
Name & Signature of the HOD	