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. The algorithm underscores its capability to ensure robust communication security through comprehensive simulations, 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 paper's main findings 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 ML and AI will drive. 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]

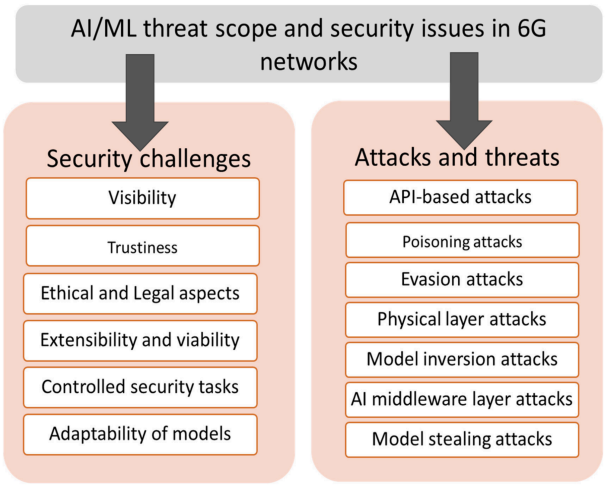

Fig.1 Security challenges and attacks in 6G networks

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 have 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.

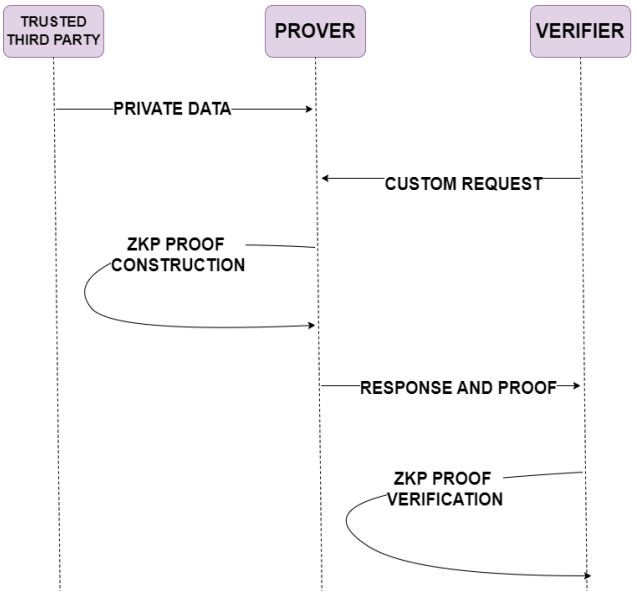

Fig.2 Zero-Knowledge Proof System

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).

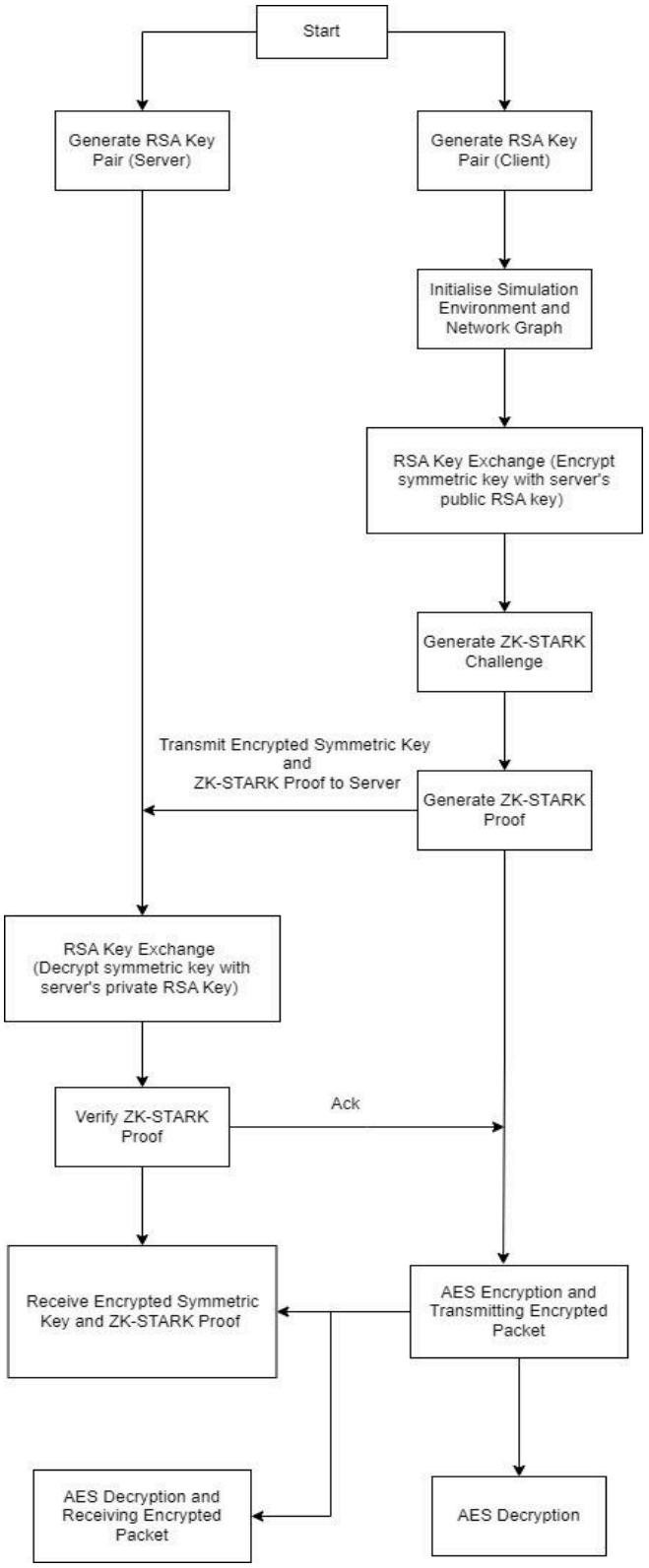

Fig.3 Framework of the proposed algorithm

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.

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.

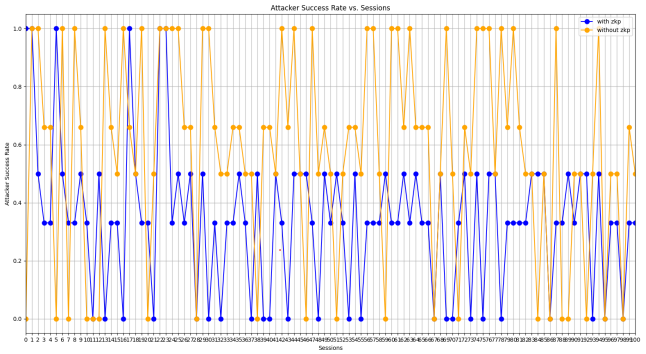

Fig.4 Simulation Results

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.

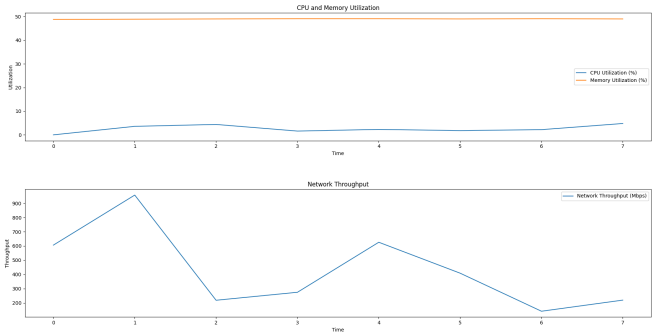

Fig.5 Idle State

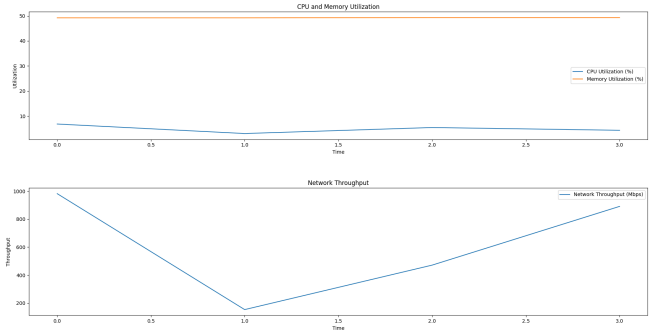

Fig.6 Busy State

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.