THE EMPLOYMENT OF MODERN SECURITY ARCHITECTURES FOR THE EMERGING 6G NETWORKS

Submitted To: Du Bing Laoshi

Dated : 2022/11/30

Submitted by: Sangeen Khan 山境
Student ID : M202261028
Subject : Digital Communications
Department of Communications Engineering,
School of Computer and Communications Engineering,
University of Science and Technology Beijing,
Beijing, China

Sangeen khan
Sangeenkhan2662@gmail.com

Abstract

With the revolution in the area of information and communication technologies based on the 5G networks, the goal of innovative techniques like the Internet of Things (IoT) was achieved. The number of devices (sensors) connected is increasing very rapidly on daily basis, and it is now the time of the Internet of Everything (IoE) instead of IoT. For such approaches, high throughput, less latency, and vast coverage are required. 6G is the optimal candidate for achieving all these characteristics to have effective communication. The increase in the number of connected devices means a huge volume of data over the internet, which will result in various security issues. The proposed article is an overview of various approaches applied for the security of 6G networks along with the future directions required to be applied for the effective privacy of clients and servers in 6G network architecture. Some important tactics like block-chain, homomorphic encryption, and multi-party computation applied for the security of 6G networks are analyzed. It was realized how one can improve the performance of modern communication systems by implementing AI-grounded decentralized security paradigms. In the end, some of the future directions were also mentioned to help the researchers in realizing the main working issues in the existing literature. Also, a comparative analysis of Paillier Encryption (PE) and Advanced Encryption Standard was carried out by analyzing the computational time of both methods.

Keywords: 6G, Internet of Things, Homomorphic encryption, Blockchain.

1. Introduction

The computer-based systems are playing a very crucial role in the progress and prosperity of human beings. Consider the smart city infrastructure, where IoT-grounded smart and intelligent sensors are deployed for providing people with effective services like smart health, intelligent transportation, and proper usage of energy resources. The integration of various approaches like artificial intelligence (AI), machine learning (ML), and federated learning (FL) assured the smooth working of smart cities. The connectivity in future communication technologies like 6G will not be limited to the only ground but will expand to sea and space. Hence, it is very essential to utilize fruitful and productive security algorithms. The very first two cellular generations—1G and 2G—made voice communication possible everywhere. Internet Access is 3G and 4G capable. Odd generations liberalized facilities for individuals while even generations established them for corporate clients. Interconnected robots and XR, the sensory web, are made possible by 5G for business sectors, and 6G will make this accessible to customers [1].

1.1 Federated Learning

To avoid communication overhead in the network to achieve low latency and high throughput, a distributed ML-based infrastructure named FL is very productive. It allows the device on the user level to utilize the collected data and build a trained model called a local model. The main server will only receive the local model without getting access to the data gathered locally. Hence, along with efficient communication, the security of the node was also ensured. It can be used for the enhancement of the overall functionality of data transmission [2]. A general overview of federated learning can be seen in figure 1.

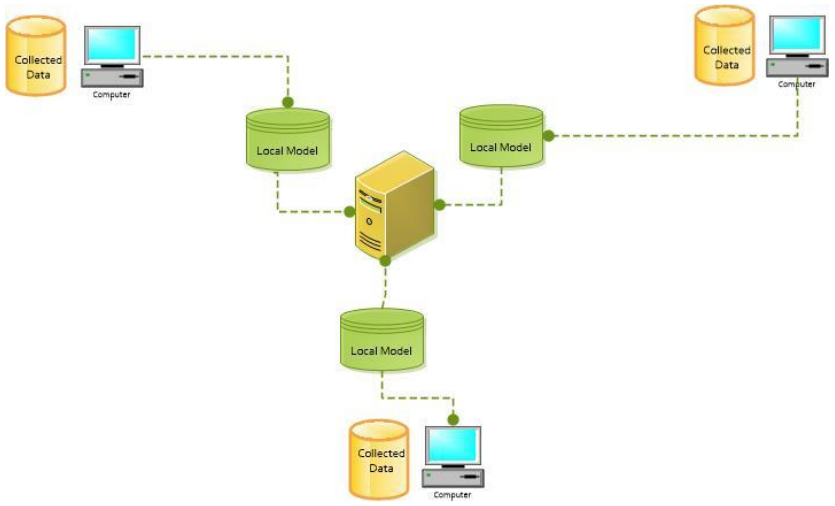

Figure 1 Federated Learning

1.2 Homomorphic Encryption

It is a very unique form of encryption that allows the computation to be carried out on the encrypted data without seeing or accessing the plaintext. It is an old concept and required high computational power to be used. But with the emergence of new systems and techniques, it is gaining more and more interest to be utilized for real-world scenarios. It can be proved very useful in the case of private and sensitive data sharing and processing [3]. The Homomorphic Encryption process is shown in figure 2.

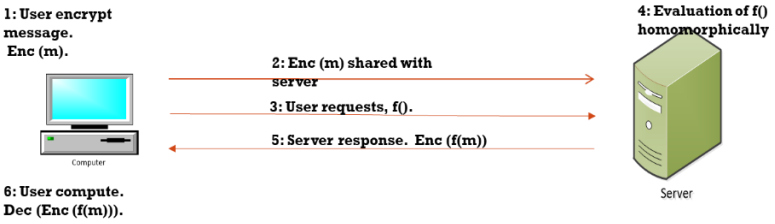

Figure 2 Homomorphic Encryption

The encryption and decryption process of the Paillier Encryption scheme (Partial HE) is given in figure 3.

```
func performEncryption(BigInteger plaintext) BigInteger {

    // n = p*q
    // p and q are two large prime numbers
    // r is a random number
    // ciphertext is c
    // c = g^m * r^n mod n^2
    BigInteger r = new BigInteger(bitLength, new Random())
    return g.modPow(plaintext, nsquare).multiply(r.modPow(n, nsquare)).mod(nsquare)
}

func performDecryption(BigInteger ciphertext) BigInteger {

    // n = p*q
    // p and q are two large prime numbers
    // r is a random number
    // ciphertext is c
    // c = g^m * r^n mod n^2
    BigInteger u = g.modPow(lambda, nsquare).subtract(BigInteger.ONE).divide(n).modInverse(n)
    return c.modPow(lambda, nsquare).subtract(BigInteger.ONE).divide(n).multiply(u).mod(n)
}
```

Figure 3 Paillier Encryption Scheme

1.3 BlockChain

A decentralized and distributed network of nodes. Information is stored in distributed blocks with digital signatures. The most efficient technique for dispersed, dependable connectivity is thought to be BC. It incorporates several characteristics, including timestamps, smart contracts, data encryption, and consensus mechanisms. The decentralization of BC technology, which eliminates the middleman between continuing transactions, is its key selling point [4]. The working of one complete transaction of blockchain can be represented in figure 4.

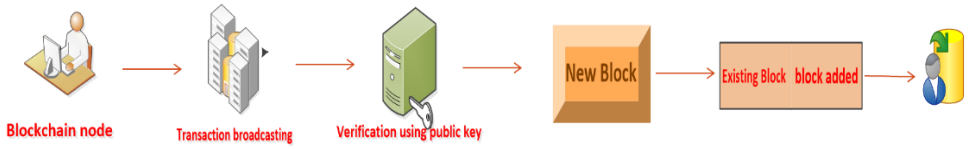

Figure 4 BlockChain

The very first block in the complete chain is known as the" Genesis Block" and the code sample for this block and the addition of a new block to the list are shown in figure 5.

```
func creatingGenesisBlock() *Block {
    return newBlock("This block is at the start of every chain of blocks", []byte{})
}

func (bc *Blockchain) AddBlock(data string) {

    // previous block is the last block in the existing list.
    // new block is the created block, whichi will be added to the previous.
    // Hash contains information about the last block.
    // data is the actual information in the block
    previous_block := bc.blocks[len(bc.blocks)-1]
    new_block := newBlock(data, previous_block.Hash)
    bc.blocks = append(bc.blocks, new_block)
}
```

Figure 5 Genesis and Addition of New Block

1.4 Multi-Party Computation

The process of MPC is somehow the same as that of HE but without or with very less computational cost. It allows the parties to perform processing of any function with their inputs

without knowing about the original data provided by them. The main difference between the HE and MPC is that the first one has a huge computational cost while the latter has a high communication cost. Both homomorphic encryption and multi-party computation can be implemented in combination to achieve an optimal and reliable security system. The implementation of MPC-grounded infrastructure with the utilization of HE techniques can be very beneficial for achieving secure computation on the encrypted data in case of multiple parties. Mouchet et al. [5] have proposed a security architecture with the employment of MPC based on the BFV encryption scheme. The system was implemented and evaluated in a semi-honest paradigm with a dishonest majority. The experimental data show that due to unique characteristics like public transcripts, they can be applied in various scenarios like cloud computing and smart-contract methodologies. It was realized that the main advantage of using HE in MPC is the reduction in communication overhead.

The main goals of the performed study are:

- To research the existing security approaches for modern communication systems.
- To study new security architectures like federated learning and homomorphic encryption.
- To identify the AI-based decentralized information security paradigms.
- To study how one can enhance the performance of 6G along with the customers' security.

The whole article is organized in the following section. Section 1 provided an overview of the selected study. A summary of the existing literature is given in section 2. The details about the various selected papers are shown in Section 3. The answers to the research questions are presented in Section 4. The overall findings of the document are given in Section 5. Section 6 is the overall summary of the conducted study.

2. Related Work

One of the most important tasks to be performed by modern network technologies is the support and feasibility of numerous connected devices. We are now living in a smart world, where intelligence is revolutionizing every aspect of our lives like health, transportation, and education. So, to handle the privacy and confidentiality of the user's data, AI and ML can be the most promising candidates. But, their implementation can result in two cases. First: they might cause damage to the user's data as they can be compromised by some malicious act. Second: their effective employment can be very helpful in performing various security procedures like intrusion detection, privacy-preserving computing, and many more. They can be used to provide security to the edge nodes in case of federated learning [6]. Due to their high speed and reliability, 6G networks can be used in the Internet of Vehicles (IoVs) for achieving high performance and accuracy. But, this will require a secure environment because of the huge number of connected devices. The authors in [7] have performed a study on the usage of the blockchain (BC) for the development of highly secure and confidential architecture to improve the security of IoVs. Based on its innovative techniques like decentralization and transparency, BC-based IoVs can be used in real-time and data-sensitive applications. But, due to its low throughput and high storage requirement, there is a need of efficient and profitable BC-grounded architecture to be developed and used.

A homomorphic encryption-grounded procedure was developed for securing the nodes in case of federated learning. The architecture will enable the main processing unit to perform the aggregation of the local model without accessing the real data of the nodes. With the employment of distributed cryptosystem, the privacy of the system was increased further by assigning a different secret key to each node in the same infrastructure. The proposed architecture was tested and evaluated in various cloud-based situations [8]. Wibawa et al. [9] have performed research on the security of medical data related to COVID-19 with the implementation of a multi-party computation based on the HE approach named Brakerski-Fan-Vercauteren (BFV). The study is very effective in providing privacy to the sensitive information about the patients shared in a federated learning atmosphere. Using this methodology, the smart decision-making model can be protected from various applied attacks. With new technological advancements in healthcare, such approaches will be very helpful to accomplish the task of smart health services.

With the increase in FL-based solutions for effective data-driven systems beyond the 5G network atmosphere, there are many security risks for secure data transmission. With the implementation of Paillier Homomorphic Encryption and differential privacy, a secure infrastructure was defined for edge intelligence in FL. Also, effective recognition and classification of anomaly-causing data sources were carried out for an enhanced performance with the assistance of the Artificial Immune Intrusion Detection System. The evaluation of the developed architecture shows that it is more feasible and reliable than the existing state-of-the-art approaches [10]. Wang et al. [11] have surveyed the applications of AI-based federated learning infrastructure for the training of models at the users' end while ensuring the privacy of a user. With the emergence of edge intelligence in the era of 6G, the existing centralized approaches are not capable of carrying out the collection of data and the development of intelligent paradigms from it. Hence, there is a need for a decentralized smart federated learning approach to enhance the abilities of edge intelligence in modern technological procedures. To accomplish this goal, various solutions and difficulties are discussed in the proposed article. The development of a secure transmission system with the integration of deep learning and homomorphic encryption is a very promising and interesting approach in this era of technological advancements. A detailed overview of the area was provided along with the effective procedure for creating privacy-preserving convolutional neural networks (CNNs). LeNet-1 CNN was enhanced using the proposed approach by the development of its secure mode. The research also focused on the upcoming issues in the area and the existing accessible methodologies [12].

A reliable system was developed for ensuring the safety of data-sharing nodes in the Internet of Things atmosphere. With the reliable combination of task decomposition and deep reinforcement learning (DRL), a secure and high-quality data-sharing approach was designed. The evaluation results show that the designed framework is more effective and can achieve high accuracy in a real-world IoT-grounded environment [13]. Dai et al. [14] have conducted a study to enhance the performance of existing federated learning architectures with the usage of deep neural networks. The research is grounded on the employment of DNN and HE for the development of a secure training framework. The resultant data show that it can achieve the same performance and efficiency as that of the already applied DNN-based methodologies.

Kaliappan et al. [15] have performed a study on the protection of information in docker images with the usage of homomorphic encryption and blockchain. The proposed system named Safe Docker Image Sharing with Homomorphic Encryption and Blockchain (SeDIS-HEB) can carry out the secure uploading, sharing, and downloading of docker images. The various facilities like authentication and protection against the DoS attacks were provided very productively with the assistance of SeDIS-HEB. Liu et al. [16] have proposed an article for the enhancement of privacy in the smart detection of metamaterials in mixtures with the employment of homomorphic encryption and convolutional neural network (CNN). For the input of the CNN, the terahertz signals were first encrypted with the help of HE and then provided to the CNN for the results. The main feature of the paradigm is that the output can only be converted into plaintext by the authorized user. It was analyzed that the developed approach can achieve an accuracy of 100% on the test sets as compared to the existing machine learning paradigms. Hamza and Minh-Son [17] have presented an architecture for the confidentiality of data obtained from a portable device for analytics. The precise combination of the CKKS HE scheme and CNN was utilized for the safety of the recorded data. The study realized that along with the protection and privacy of sensitive data, there is a need for a such system that can also enhance the performance of ML-grounded analytics approaches. An overview of various privacy procedures was provided which are also applicable to the upcoming 6G techniques. The research was conducted to ensure the secure sharing of images on vulnerable networks with the exploitation of the Elliptic Curve ElGamal (EC-ElGamal). The developed paradigm is more reliable and efficient than the existing approaches due to its shorter key. The various attacks like Isomorphism were avoided with the selection of Elliptic curve parameters. The performance of encryption and decryption was greatly improved by the reduction in computation overhead with the employment of this procedure [18].

With the uncovering of numerous 6G-grounded reliable procedures like network openness, the risk of various security threats increases very rapidly. With such high connectivity, it is very challenging to secure the confidentiality of the end users along with different authentication. There is a need for a strong and feasible cryptographic system to be applied in such scenarios. This architecture should be capable of providing security against innovative and high-quality computers such as quantum computing [19]. The main focus of the 6G networks is on intelligence connectivity instead of only connecting things. Rahman and Hossain [20] have proposed a security architecture for the detection and recognition of different security threats with the implementation of deep learning (DL) for software-defined security (SDS). Using security function virtualization (SFV), the architecture can spot, confine, and cut off various threats very efficiently. The study of cyber and physical units is gaining more and more interest with the development of modern networks. Some upcoming challenges were also analyzed in the study. The modern 6G networks will serve as a turning point for efficient connectivity among people, objects, and data. These developments can be made possible with the implementation of various existing methodologies like quantum cryptography, artificial intelligence, and machine learning, but with some smart and intelligent changes in the security infrastructure of all these paradigms. The innovative privacy algorithms should be reliable and productive in meeting the requirements of end users in the upcoming high-speed and low-latency networks [21].

3. Methodology

The proposed article is an overview of various security issues in 6G networks and the state-of-the-art approaches applied to resolving these vulnerability concerns. With increasing connectivity and the generation of a huge volume of data in modern networking techniques, the privacy of the user's data is gaining more and more interest. Some of the recently developed architecture for accomplishing this goal are mentioned in this document.

3.1 Research Strings

The existing literature was studied by using some strings as given below:

- "Federated Learning" AND "6G".
- "Multi-party computation" AND "Privacy-preserving computing".
- "Homomorphic encryption" AND "6G".
- "Homomorphic encryption" AND "Blockchain".

3.2 Research Questions

The study is mainly focused on the three questions as shown in table 1.

Table 1 Research Questions

Q. No.	Questions	Explanation
1	Why Federated Learning is an effective platform for 6G?	The main focus of the question is to realize the employment of FL for enhancing the performance of AI-grounded smart systems in various 6G-grounded applications like smart health.
2	How HE can enhance the security in 6G networks?	The goal is to analyze the enhancement in the security of diverse data nodes in the IoE-based atmosphere.
3	How can blockchain be integrated with homomorphic encryption?	The focus of this research question is the integration of blockchain with HE to achieve high-performance encryption.

3.3 Selected Papers

The total number of papers selected for the article along with their year of publication are presented in figure 6.

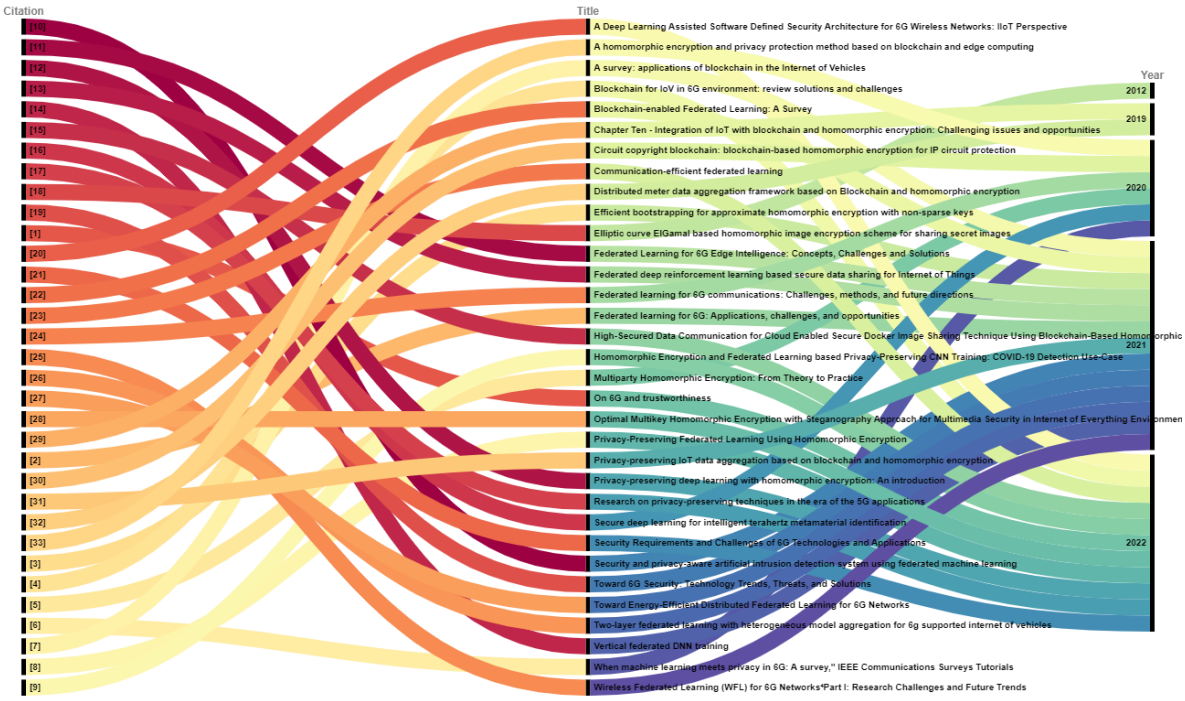

Figure 6 Selected Papers

3.4 Searched Repositories

The papers selected from various online repositories are presented in figure 7.

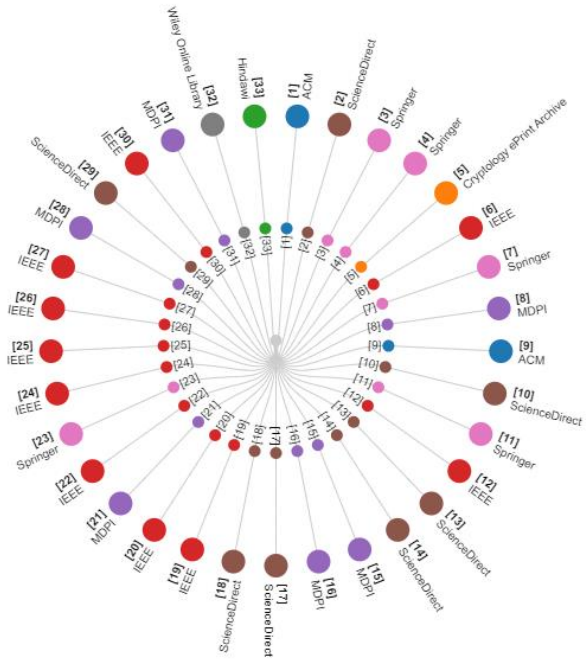

Figure 7 Searched Repositories

4. Results and Discussion

This section provided an overview of the selected research papers along with detailed answers to the research questions. The findings of the proposed study are then presented in a separate section.

4.1 Percentages of papers

The papers identified from various resources along with their percentages are given in figure 8.

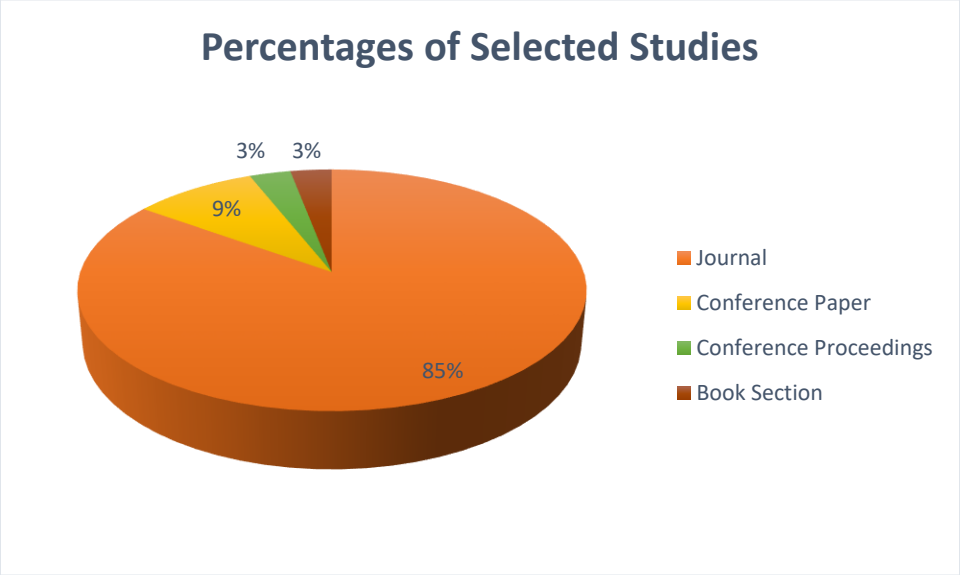

Figure 8 Percentages of Studies

4.2 Year-wise selection of papers

The number of studies selected from different years is shown in figure 9.

Figure 9 Year-Wise Selection of Papers

Why Federated Learning is an effective platform for 6G? (RQ1)

As compared to a centralized processing system, FL can perform resource allocation in a distributed manner and can perform various tasks like analysis of the data without transmission to the main station [2]. It is very effective for training the AI-based models locally without making the data public [8]. The performance of edge intelligence in smart systems can be enhanced with the employment of FL [11]. The selection of efficient and high-quality nodes in federated learning can result in secure and reliable data-sharing [13]. FL can be used in combination with DNN very productively and efficiently for the training of a model [14]. The security of federated learning can be greatly improved with the utilization of block-chain based cryptographic systems [22]. The precise and accurate utilization of distributed intelligence in the era of 6G can be accomplished with the employment of federated learning [23]. It can be employed very productively for enhancing the performance of various wireless platforms and is one of the best candidates for achieving the goal of pervasive AI in the 6G era [24]. With the assistance of FL-based architecture, it is very convenient to deal with and manage the big data produced by wireless-connected smart devices [25]. It is very beneficial for accurate training in edge intelligence along with increasing the confidentiality and privacy of sensitive data in a network [26]. Various difficulties related to IoT-based sensors and healthy utilization of energy assets can be resolved using federated learning techniques [27].

How HE can enhance the security in 6G networks? (RQ2)

The homomorphic encryption approach can be used to reduce the communication in the multi-party computation procedure and hence can secure the data along with increasing the speed of the framework [5]. It can be applied for the privacy of various features of the model in federated learning, which in turn can improve the overall functionality of a system [8]. The privacy of an intelligence model in FL can be achieved with the precise implementation of HE by encrypting sensitive medical data [9]. It can be applied very efficiently for ensuring the privacy of deep learning-based approaches [12]. The integration of FL and HE can enable the secure training model implementation in the IoT atmosphere [14]. The employment of HE can improve the privacy of data contained in the docker images during uploading, sharing, and downloading [15]. The integration of HE and CNN can provide effective confidentiality to the data and intelligent system used for the decision-making process [16]. Efficient privacy-preserving approaches can be developed with the integration of homomorphic encryption and CNN [17]. The performance of HE can be enhanced with the usage of Elliptic Curve ElGamal for securing the sharing of images with the help of a shorter key [18]. The precise integration of homomorphic encryption with other ciphering techniques like steganography can improve the security of multimedia data in the Internet of Everything (IoE) [28].

How can blockchain be integrated with homomorphic encryption? (RQ3)

With the existing centralized architectures, the data stored on the server is vulnerable to various attacks like privacy leakage. Shrestha and Kim [29] have conducted a study on the blockchain-grounded IoT paradigm for solving the issues of privacy leakage in integration with homomorphic encryption. These techniques can be very effective in achieving the goal of privacy-preserving

computing. Blockchain and smart contracts have created a homomorphic encryption-based computational formula; secondly, the procedures for creating a blockchain, encrypting and decrypting a homomorphic chain, and creating a smart contract are created [30]. Loukil et al. [31] have presented PrivDA, an IoT data aggregation system that protects privacy that relies on blockchain and homomorphic encryption. Every data user in the suggested method can build a smart contract and broadcast both the terms of the agreement and the desired IoT records. As a consequence, the smart contract gathers all prospective data suppliers who can fulfill the user's demand into one group and selects one aggregator, whose job it is to calculate the outcome that the group has required via homomorphic computing. Wang et al. [32] have suggested an architecture for meter data aggregation that is distributed, safe, and protects privacy, supported by Blockchain and homomorphic encryption (HE) technology. A nested Blockchain platform aggregates and verifies meter readings. To safeguard the confidentiality of specific meter data objects throughout the clustering procedure, HE technology is employed on top of the Blockchain architecture. The proposed study focused on the enhancement of the security of an end-user with the employment of blockchain methodology. The performance of the developed system was increased with the implementation of the Paillier encryption algorithm which supports the additive property of homomorphic encryption [33].

5. Findings of the article and Future directions

The important observations of the performed study are given below:

- The main goal of the 6G is to bring enhancement in the current communication era both in connectivity and speed.
- Artificial intelligence and information security are the two most important enablers of the 6G technology.
- The decentralized networking architecture can play a very important role in achieving low latency and high performance.
- AI-grounded systems like federated learning can be integrated with homomorphic encryption to resolve various security vulnerabilities.
- The integration of blockchain and homomorphic encryption can help in the solution of communication and computational issues.

Some of the improvements needed in the existing approaches are:

- Work should be done on the selection of efficient and effective nodes in the federated learning environment.
- There is a need for investigation into the computational and time complexity of homomorphic encryption systems. The computational time comparison of the Paillier Encryption Scheme (Partial HE) and Advanced Encryption Standard (AES) is given in figure 10. The size of the plain text is in the order of Text 1 < Text 2< Text 3 < Text 4 < Text 5.

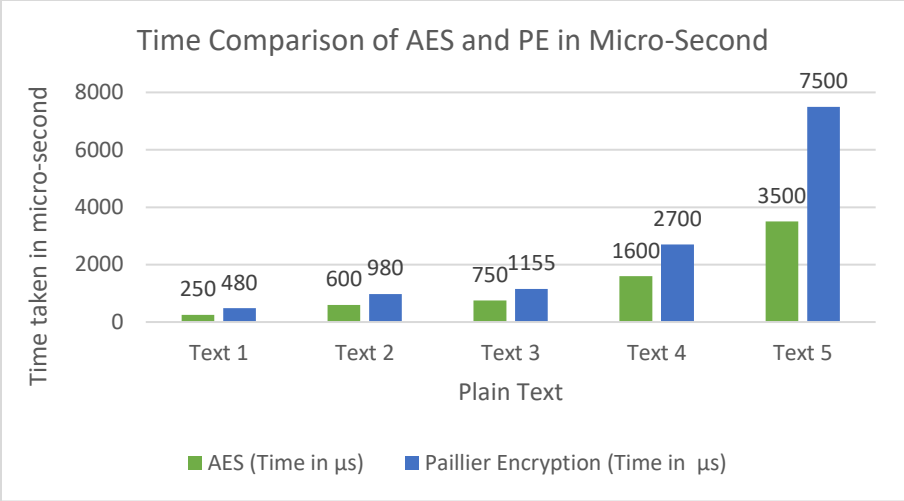

Figure 10 Comparison of PE and AES

- Research should be carried out for resolving the issues like storage and transparency in the blockchain paradigms.

6. Conclusion

The world is now moving to explore unique aspects like intelligence connectivity, space-air-grounded integrated network, and many more with the employment of 6G. But, due to high connectivity and AI-governed systems, the issue of security is one of the major concerns of today's technological advancements. There is a need for an efficient and reliable procedure to be developed for the security of end-user in the smart atmosphere. The article summarizes some of the precise infrastructures employed in the area of research. It is necessary to create a secure system, which not only provides privacy but also enhances the computational power of the paradigm.

References:

[1] G. P. Fettweis and H. Boche, "On 6G and trustworthiness," *Communications of the ACM,* vol. 65, no. 4, pp. 48-49, 2022.

[2] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor, and S. Cui, "Federated learning for 6G: Applications, challenges, and opportunities," *Engineering,* 2021.

[3] J.-P. Bossuat, C. Mouchet, J. Troncoso-Pastoriza, and J.-P. Hubaux, "Efficient bootstrapping for approximate homomorphic encryption with non-sparse keys," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2021, pp. 587-617: Springer.

[4] K. Shah, S. Chadotra, S. Tanwar, R. Gupta, and N. Kumar, "Blockchain for IoV in 6G environment: review solutions and challenges," *Cluster Computing,* vol. 25, no. 3, pp. 1927-1955, 2022/06/01 2022.

[5] C. Mouchet, J. R. Troncoso-Pastoriza, and J.-P. Hubaux, "Multiparty Homomorphic Encryption: From Theory to Practice," *IACR Cryptol. ePrint Arch.,* vol. 2020, p. 304, 2020.

[6] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Communications Surveys Tutorials,* vol. 22, no. 4, pp. 2694-2724, 2020.

[7] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: applications of blockchain in the Internet of Vehicles," *EURASIP Journal on Wireless Communications and Networking,* vol. 2021, no. 1, p. 77, 2021/04/07 2021.

[8] J. Park and H. Lim, "Privacy-Preserving Federated Learning Using Homomorphic Encryption," *Applied Sciences,* vol. 12, no. 2, p. 734, 2022.

[9] F. Wibawa, F. O. Catak, M. Kuzlu, S. Sarp, and U. Cali, "Homomorphic Encryption and Federated Learning based Privacy-Preserving CNN Training: COVID-19 Detection Use-Case," in *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*, 2022, pp. 85-90.

[10] K. S. Kumar, S. A. H. Nair, D. G. Roy, B. Rajalingam, and R. S. Kumar, "Security and privacy-aware artificial intrusion detection system using federated machine learning," *Computers Electrical Engineering,* vol. 96, p. 107440, 2021.

[11] H. Wang, J. Hu, C. Xing, and L.-J. Zhang, "Federated Learning for 6G Edge Intelligence: Concepts, Challenges and Solutions," in *International Conference on AI and Mobile Services*, 2021, pp. 99-112: Springer.

[12] A. Falcetta and M. Roveri, "Privacy-preserving deep learning with homomorphic encryption: An introduction," *IEEE Computational Intelligence Magazine,* vol. 17, no. 3, pp. 14-25, 2022.

[13] Q. Miao, H. Lin, X. Wang, and M. M. Hassan, "Federated deep reinforcement learning based secure data sharing for Internet of Things," *Computer Networks,* vol. 197, p. 108327, 2021.

[14] M. Dai, A. Xu, Q. Huang, Z. Zhang, and X. Lin, "Vertical federated DNN training," *Physical Communication,* vol. 49, p. 101465, 2021.

[15] V. K. Kaliappan, S. Yu, R. Soundararajan, S. Jeon, D. Min, and E. Choi, "High-Secured Data Communication for Cloud Enabled Secure Docker Image Sharing Technique Using Blockchain-Based Homomorphic Encryption," *Energies,* vol. 15, no. 15, p. 5544, 2022.

[16] F. Liu *et al.*, "Secure deep learning for intelligent terahertz metamaterial identification," *Sensors,* vol. 20, no. 19, p. 5673, 2020.

[17] R. Hamza and D. Minh-Son, "Research on privacy-preserving techniques in the era of the 5G applications," *Virtual Reality Intelligent Hardware,* vol. 4, no. 3, pp. 210-222, 2022.

[18] L. Li, A. A. Abd El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," *Signal Processing,* vol. 92, no. 4, pp. 1069-1078, 2012.

[19] D. Je, J. Jung, and S. Choi, "Toward 6G Security: Technology Trends, Threats, and Solutions," *IEEE Communications Standards Magazine,* vol. 5, no. 3, pp. 64-71, 2021.

[20] M. A. Rahman and M. S. Hossain, "A Deep Learning Assisted Software Defined Security Architecture for 6G Wireless Networks: IIoT Perspective," *IEEE Wireless Communications,* vol. 29, no. 2, pp. 52-59, 2022.

[21] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," *Sensors,* vol. 22, no. 5, p. 1969, 2022.

[22] C. Li, Y. Yuan, and F.-Y. Wang, "Blockchain-enabled Federated Learning: A Survey," in *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*, 2021, pp. 286-289: IEEE.

[23] K. Kishor, "Communication-efficient federated learning," in *Federated Learning for IoT Applications*: Springer, 2022, pp. 135-156.

[24] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," *China Communications,* vol. 17, no. 9, pp. 105-118, 2020.

[25] P. S. Bouzinis, P. D. Diamantoulakis, and G. K. Karagiannidis, "Wireless Federated Learning (WFL) for 6G Networks[4]Part I: Research Challenges and Future Trends," *IEEE Communications Letters,* vol. 26, no. 1, pp. 3-7, 2021.

[26] X. Zhou, W. Liang, J. She, Z. Yan, I. Kevin, and K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 6, pp. 5308-5317, 2021.

[27] S. A. Khowaja, K. Dev, P. Khowaja, and P. Bellavista, "Toward Energy-Efficient Distributed Federated Learning for 6G Networks," *IEEE Wireless Communications,* vol. 28, no. 6, pp. 34-40, 2021.

[28] I. Abunadi *et al.*, "Optimal Multikey Homomorphic Encryption with Steganography Approach for Multimedia Security in Internet of Everything Environment," *Applied Sciences,* vol. 12, no. 8, p. 4026, 2022.

[29] R. Shrestha and S. Kim, "Chapter Ten - Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities," in *Advances in Computers*, vol. 115, S. Kim, G. C. Deka, and P. Zhang, Eds.: Elsevier, 2019, pp. 293-331.

[30] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, "Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection," *IEEE Transactions on Emerging Topics in Computing,* vol. 9, no. 3, pp. 1410-1420, 2020.

[31] F. Loukil, C. Ghedira-Guegan, K. Boukadi, and A.-N. Benharkat, "Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption," *Sensors,* vol. 21, no. 7, p. 2452, 2021.

[32] Y. Wang, F. Luo, Z. Dong, Z. Tong, and Y. Qiao, "Distributed meter data aggregation framework based on Blockchain and homomorphic encryption," *IET Cyber-Physical Systems: Theory Applications,* vol. 4, no. 1, pp. 30-37, 2019.

[33] X. Yan, Q. Wu, and Y. Sun, "A homomorphic encryption and privacy protection method based on blockchain and edge computing," *Wireless Communications Mobile Computing,* vol. 2020, 2020.