

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>

Research Paper

Open Access

Two Way Authentication with Attribute Based Encryption to Increase Security of 5G Networks

Kamaldeep Kaur^{1*}, Sarpreet Kaur², Sabhyata Uppal Soni³^{1*}Research Scholar, UIET, Panjab University, India. E-mail: kamal.0902@gmail.com²Assistant Professor, EEE, UIET, Panjab University, Chandigarh, India. E-mail: sarpreetdua@yahoo.co.in³Assistant Professor, EEE, UIET, Panjab University, Chandigarh, India. E-mail: sabhyatauiet@gmail.com

ABSTRACT

The direction of mobile communication technology development is toward 5G technology. It is feasible to "wirelessly" control production control systems, such as power monitoring systems, thanks to their low latency and high reliability properties. Users in the power industry can establish specialised "business private network" services using 5G network slicing technologies to better fulfil the varied needs of power grid services. The fully Homomorphic encryption (FHE) is adaptable to perform all kinds of calculation on the data that the network has contained. The FHE facilitates the execution of all kinds of operations on encrypted data without performing decryption. The application of FHE is essential to keep the network infrastructure secure. The calculations are outsourced on the secret data to the server with the secret key which assists in decrypting the result of calculation. This work suggests an innovative framework for enhancing the security of network. The proposed model is implemented in MATLAB and results are analyzed in terms of energy consumption, time and resource consumption.

Keywords: 5G, Security, Secure Channel, FHE, Diffie-Helman

1. Introduction

The exponential surge in data and device usage within wireless networks presents a formidable challenge to existing infrastructure. To address this escalating demand, the next phase of mobile cellular communication and networking, known as 5G, has emerged. This revolutionary technology incorporates elements such as edge computing, Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Device-to-Device (D2D) communications. The International Telecommunication Union (ITU) has delineated three primary application scenarios for 5G: Ultra-reliable and Low Latency Communications (URLLC) [1][2], Massive Machine-Type Communications (mMTC), and Enhanced Mobile Broadband (eMBB). Contrasted with the 4G's maximum data rate of 10 gigabits per second, enhanced mobile broadband offers speeds that are a hundredfold faster. In Massive Type Communications, a Base Station (BS) plays a crucial role in managing a large number of devices meant for the Internet of Things (IoT) ecosystem. This oversight is essential for ensuring efficient communication and coordination among these devices. Furthermore, in critical scenarios such as vital machine communications and vehicle-to-everything (V2X) interactions, high bandwidth and low latency are paramount to guarantee reliability and responsiveness [3][4].

The 5G network consists of two primary components: the Radio Access Network (RAN) and the Core Network (CN). Within the Core Network, key functions include the Authentication Server Function (AUSF), User Plane Function (UPF), Session Management Function (SMF), and Access and Mobility Management Function (AMF). Communication within the RAN involves Mobile Entities (MEs) and g-Node Base Stations (gNBs). Before a ME can establish a connection to the 5G CN, the AMF initiates mutual authentication with the AUSF [5][6]. Additionally, the 5G system facilitates integration with other non-3GPP access networks through the Non3GPP Interworking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNGF), alongside 5G NR and 4G LTE. WLANs, a common non-3GPP network, are frequently utilized in everyday scenarios.

5G technology enables D2D communications, enhancing network resource utilization by allowing direct communication between nearby devices without relying on base stations to relay messages. The vehicular network within the 5G system is another critical component. In addition to connecting to the 5G Core Network via a 5G wireless access network, vehicles can also connect to Road Side Units (RSUs) to access road information. Vehicular networks play a pivotal role in achieving autonomous driving [7][8]. With the integration of various communication networks such as Wireless Local Area Networks (WLAN), Long Term Evolution (LTE), Internet of Things (IoT), Vehicular Ad-hoc Network (VANET), and New Radio (NR), 5G exhibits exceptional versatility and heterogeneity. Various Radio Access Technologies (RAT) are utilized across these networks, including the WLAN 802.11 standards, WiMAX, and Evolved Universal Terrestrial Radio Access (E-UTRA). However, to meet the demand for high data access rates and network capacity in 5G, networks deploy

a large number of small Access Points (APs) because of the limited signal penetration of high-frequency waves used in the technology. The ongoing densification of the network and increasing heterogeneity pose challenges for supporting the mobility of Mobile Equipment (ME) [9][10].

1.1 Handoff Mechanism in 5G

Handoff is indispensable in any mobile network with a distributed access design, ensuring uninterrupted provision of network services, including Quality of Service (QoS), connection maintenance between Mobile Equipment (ME) and Base Stations (BS), and security and privacy protection when ME switches between radio networks or cells. In 5G networks, characterized by massive BS deployment and ongoing network heterogeneity, handover is essential to meet the escalating demand for mobile data. However, 5G networks encounter significant challenges with handover due to new technologies [11][12]. For instance, seamless handover among diverse networks necessitates a highly compatible handover system. Moreover, the deployment of numerous small cells leads to frequent handovers, occurring approximately every 11.6 seconds due to the limited penetrability of millimetre-wave signals and diminishing cell coverage. Additionally, facilitating seamless mobility assistance across networks with different Radio Access Technologies (RATs) poses a significant difficulty. Consequently, improving handoff performance in 5G networks is imperative to address these challenges effectively.

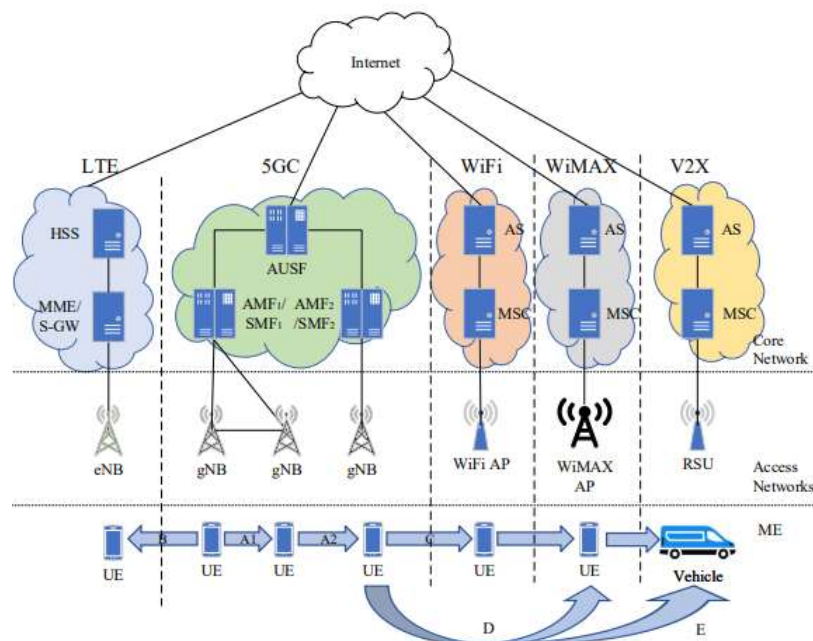


Fig. 1. Handoff scenarios in 5G networks

Figure 1 illustrates various handoff scenarios in 5G, involving six key network entities: Mobile Equipment (ME), source Base Station (BS), target Base Station (BS), source Mobile Service Controller (MSC), target Mobile Service Controller (MSC), and Authentication Server (AS). These entities can be categorized into three groups based on their capabilities and deployment locations: ME, Radio Access Network (RAN), and Core Network (CN). ME represents the hardware requiring seamless 5G network connectivity. Given the diversity of 5G networks, MEs can encompass devices such as laptops, smartphones, wearable technology, automobiles, sensors, and more. The handoff process often experiences significant delays due to the limited resources, including processing capacity, of these devices [13][14]. In a mobile network, RAN facilitates radio access service for ME through various types of BSs, such as the gNB of 5G, the e-Node Base Station (eNB) of LTE, the Access Point (AP) of WiMAX, and the Road Side Unit (RSU) of VANET. During handover within the Core Network (CN), key entities include the Mobility Management Entity (MME) in LTE and the AMF in 5G, along with the Authentication Server Function (AS), like the Home Subscriber Server (HSS) in LTE and the AUSF in 5G. The MSC, responsible for user mobility management and handover authentication, plays a crucial role. In a 5G scenario, when an ME moves from a source gNB to a target gNB or when a source gNB cannot provide better data or voice services than another gNB, the ME initiates handoff by sending a request to the target gNB, ensuring communication continuity [15][16]. Only after subscription service checking and security authentication by the target gNB, AMF, and UDM, can the ME connect to the target BS for uninterrupted service.

2. Literature Review

L. Mei, et.al (2022) conducted research on the feasibility and accuracy of real-time mobile handoff and bandwidth predictions in both 5G and 4G/LTE networks [18]. To accomplish this, the researchers collected extensive, consecutive traces from public transit networks containing abundant bandwidth, channel, and

contextual data. Subsequently, they developed recurrent neural network models to extract temporal patterns of bandwidth evolution in fixed-route mobility scenarios. The presented models consistently outperformed traditional methods in univariate and multivariate bandwidth prediction. Specifically, the proposed model demonstrated an average improvement of 15.28% for next-second bandwidth prediction in 4G traces and 15.37% in 5G traces, as measured by Mean Absolute Error (MAE). Furthermore, to enhance application performance in realistic 5G environments, the study introduced a novel challenge of handoff prediction between 4G and 5G networks coexisting. Utilizing a recent 5G dataset, they developed classification and regression-based prediction models capable of forecasting handoffs between 4G and 5G networks with over 80% accuracy.

N. Zohar, et.al (2022) proposed to use proximity-based clusters as nomadic cells connected with Aerial Access Networks (AANs) to facilitate a large number of highly mobile devices in 5G and beyond networks [19], while mitigating the load generated by quick handover requests. The mobile devices were divided into proximity-based clusters using a two-level hierarchical partitioning technique to create these nomadic cells. The handover rate anticipated for 5G and beyond networks was not supported by previous distributed mobility management solutions due to their insufficient efficiency. For real-time services, prior group-based approaches were unsuitable due to their high computing complexity. The suggested approach, in contrast to these others, was scalable in terms of the number of devices. In addition, the establishment of a mobility group brought up pragmatic challenges that prior schemes ignored, in addition to security and privacy concerns.

V. K. Shaw, et.al (2020) investigated a system model of two-tier cellular networks utilizing deterministic geometry [20]. Their study focused on 5G small-cell networks, wherein they analyzed the signal-to-interference-noise ratio (SINR), coverage probability, and handoff rate based on the distance between vehicles and small-cell base stations. They developed a handoff algorithm considering factors like cell radius, distance, and SINR to minimize the handoff rate. Comparing their results with small cell base station complexes arranged using the Poisson Point Process (PPP), they found comparable performance. Their approach provided a low-complexity solution for addressing handoff issues in 5G small-cell networks.

C. Roy, et.al (2021) explored the application of a 5G-enabled Intelligent Transportation System (ITS) within the context of road transportation, focusing on Safe-aaS [21]. They proposed a service handoff system among various service providers aimed at providing end users with safety-related decisions. The researchers devised a method to calculate the profit of the nearest Service Supply Point (SSP) willing to provide services to the end user, based on the reputation and profit of the SSP initially registered for services by the end users. These interactions among SSPs were modeled as a cooperative coalition game, with SSPs assuming player roles. Through a comprehensive simulation-based analysis, Safe-Passé was found to improve the ratio of end users served to total end users by 4.19% and 3.65%, respectively, compared to current handoff methods such as UCH and VHO.

N. Sharghivand, et.al (2023) suggested the Online Service Handoff Mechanism (OSHM), which provided a mobile user with a dynamic method to transfer a virtual machine (VM) or container from the current serving 5Glet to a neighbouring 5Glet [22]. The suggested path planning algorithm achieved polynomial time complexity due to the label correction mechanism employed. To prevent false reporting of unknown parameters, a payment determination function was incorporated into OSHM. The scholars discussed the theoretical properties of the proposed procedure in achieving system equilibrium and ensuring accuracy. Furthermore, they conducted a comprehensive evaluation through various experiments, demonstrating the effectiveness of OSHM compared to other benchmarks in terms of workload, handoff time, energy consumption, and other metrics. Experimental results indicated that OSHM outperformed other algorithms, achieving at least a 61% reduction in average workload, a 33% decrease in average handoff time, and a 29% reduction in average energy consumption.

A. I. Mbulwa, et.al (2024) presented a self-optimization technique for the three crucial handover control parameters (HCPs) of time-to-trigger, hysteresis, and threshold. To identify the ideal values for these HCPs, a comprehensive variety of criteria was taken into account in the suggested methodology [23]. These variables comprised the user's direction and speed (mobility profile), the received power of reference signals (channel conditions), and the handover procedure latency and frequency of the synchronization signal (representing system parameters). The study developed a framework through analytical discussions to attain the best HCPs in order to decrease handovers, lessen handover failures, mitigate ping-pong effects, and maintain good throughput performance. Moreover, by considering channel, user, and system parameters, cell-specific Handover Control Parameters (HCP) optimization was facilitated, allowing the implementation of this method with any of the measurement events specified in the 3rd Generation Partnership Project (3GPP) release 16 for 5G. The study demonstrated that simultaneous self-optimization of Threshold, Hysteresis, and Time-To-Trigger could lead to significant improvements in handover performance.

Y. Zhang, et.al (2024) presented RUSH, an authentication mechanism for 5G HetNets that is both robust and universally seamless. Using the tamper-resistance of blockchains and the trapdoor collision property of chameleon hash functions, RUSH enabled anonymous mutual authentication with key agreement for handovers [24]. As demonstrated by the transition between 5G new radio and non-3GPP access, RUSH obtained universal handover authentication for all the various mobility situations, irrespective of the reliability of non-3GPP

access and the coherence of the core network. Additionally, RUSH accomplished robust tracking, known randomness secrecy, perfect forward secrecy, master key forward secrecy, and key escrow freeness. Rush's resistance to several types of assaults was demonstrated by the formal security proofs based on the BAN-logic and the formal verification based on AVISPA. Thorough analysis and comparisons revealed that RUSH performed better than other methods in terms of processing and communication efficiencies.

H. Zhang, et.al (2019) suggested an anchor-based multi-connectivity (MC) architecture and derived concise expressions for handover probabilities (HOPs) through stochastic geometry analysis in user-centric networks (UCN). The aim was to minimize handover costs resulting from network densification [25]. In the MC scenario where a user connects to multiple access points (APs), the optimal AP is selected as the handover anchor to manage the control-plane, thus reducing the handover rate. By modeling APs as a Poisson point process, HOPs were quantified for a typical user moving in an irregular UCN at a constant speed and in random directions. Simulation and analytical results showed that the control-plane HOP could be reduced by over 40% compared to conventional handover techniques in LTE systems.

3. Research Methodology

This research work is based on to increase security of 5G networks. The proposed methodology has various phases which are explained below: -

1. Original identity transmission and secure channel generation: - At initial stage, the user sends the original identity to the Key Identity Provider and creates a secure channel. For this, Diffie-Hellman (DH) algorithm is implemented. DH is considered as a mathematical algorithm which assists two systems in generating an identical secret whose transmission is done on both systems. However, these systems have not any communication among one another. The transmitted secret is employed for broadcasting a cryptographic encryption key in a secure manner. This work aims to encrypt the traffic amid 2 systems. This algorithm is effective for encrypting the data on web on the basis of Secure Socket Layer (SSL) or Transport Layer Security (TLS). Moreover, this algorithm makes the deployment of Secure Shell (SSH) protocol. This protocol is employed for exchanging the key securely for encrypting the data. A shared secret which is also known as Key Encryption Key (KEK) is considered for exchanging this secure transmission. Thereafter, the transmitted secret helps to encrypt the symmetric key to achieve safe transmittal. This process is initialized by generating a private key on every side of the correspondence. Every end concentrates on generating a public key that is obtained as the derivation of the private key. The next task is to exchange the public keys amid both systems. Hence, it provides own private key and the other public key of systems to each side of the correspondence. After completing the key sharing, the process is executed further. Consequently, this algorithm leads to generate a shared key as identical cryptographic key whose transmission is done via each side. Afterward, the mathematical operation is deployed against the private key and other side's public key for acquiring a value. In the end, cryptographic key assists in encrypting the traffic. The Diffie-Hellman algorithm often utilizes a shared secret for encrypting a symmetric key for one of the symmetric algorithms and transmitting it in secure manner. The inaccessible end is exploited in this algorithm for decrypting it with the shared secret. At the completion of transmitting a symmetric key securely, the data is encrypted and a communication is established securely.

2. Virtual Identity Generation and Transmission: - the key identity provider provides an identity provider and private key to the user. Moreover, it sends a public key and identity to the 5G. The fourth stage employs the HE technique so that the data is encrypted. The HE is a property of an encryption methodology which is robust to be executed in the encrypted information (ciphertexts) and to preserve the actual operation outcomes on the underlying clear text operands. This approach is consisted of a number of applications and it is deployed for carrying out computations on encrypted data on the basis of data which is concealed from it. Assume a scenario in which a client is there along with a relatively weak computing device and a server which is comprised of robust computing resources. Moreover, considers that a client focuses on outsourcing its data to the remote server so that computing results are obtained and performing computations over the data. The HE approach is provide suitable for this process. It helps a client in generating a ciphertext of its secret data and transmitting it to a server. Afterward, a ciphertext of the computation result is provided to the server. For this, the homomorphic evaluations are carried out on the ciphertext of client and this ciphertext is returned to the client. At last, the client is able to decrypt the evaluated ciphertext, and attains the computation result. There is not any association amid the computation cost for a client and the size of a delegated function. HE approach is capable of handing the ciphertext for users without key, and in this process, no information related to plaintext is revealed. This attribute is effective for protecting the security of information and enhancing the efficacy to process the information. More specifically, in case an encryption function f results in satisfying

$$f(a) + f(b) = f(a + b)$$

It is considered that it has additive homomorphism, and in case it satisfies

$$f(a) * f(b) = f(a * b)$$

This implies that this function contains multiplicative homomorphism. The Homomorphic encryption (HE) is executed for managing ciphertext and to retrieve, calculate and compute the ciphertext within the 5G directly. Hence, the output is provided to customers as ciphertext. There is not any necessity of regular encryption and decryption amid the 5G and customers in this approach. It results in mitigating the message and computational overhead. There are some properties of this approach. This procedure is executed in seven stages: original identity transmission, secure channel generation, Identity provider and private key transmission, public key and identity transmission, data encryption, data transmission and data storage in 5G.

The key sizes for fully homomorphic encryption (FHE) schemes commonly used in practical applications can vary, but they are generally larger than those of traditional encryption schemes due to the additional requirements for supporting computations on encrypted data. Key sizes are influenced by factors such as the specific FHE algorithm, the desired security level. In this research work we have used 150-bit long key for the encryption and decryption. The Fully homomorphic encryption keys is bit long than traditional algorithms due to which it has less chances of attacks and also less execution time.

3. Data Security: - In the next stage, the encrypted data is transmitted to the 5G. In the last stage, the 5G attains the public key and identity from the key identity provider and private key from user. Then it focuses on decrypting both the keys and storing the data. Homomorphic encryption (HE) is an effective method to perform data encryption and decryption in diverse phases which are described as:

3.1. Data Encryption: The data owner focuses on encrypting their sensitive data. For this, a homomorphic encryption method is employed. This method further has diverse kinds namely partially homomorphic encryption or fully homomorphic encryption. The next task is to transmit and store the encrypted data in a secure way for which there is not any necessity of decrypting the data.

3.2. Data Processing: A third party, like a service provider or an application, is capable of executing calculations on the encrypted data. HE method is composed of particular mathematical operations such as addition and multiplication, which can be executed on the encrypted data.

4. Data Decryption: - After completing the selected computations on the encrypted data, the results are generated in encrypted form. The data owner, who is responsible for possessing the decryption key, becomes able to decrypt the result for attaining the final output. Homomorphic encryption is consisted of diverse levels for determining the kinds of operations which are suitable to preserve the encryption. Moreover, partially homomorphic encryption methods namely Paillier encryption etc. are also available. But, these method comprises only restricted number of operations such as addition and multiplication, and fully homomorphic encryption methods, namely TFHE, BFV, CKKS can be deployed to carry out complicated computations.

4. Result And Discussion

This research work is implemented in MATLAB using the mathematical tool box. It is an interactive program which provides numerical computation and visualization of data. With the help of its programming capabilities it provides tool which is very useful for all areas of science and engineering. Image Processing Toolbox chains a various set of image and their types, together with high forceful range, embedded ICC profile, topographic and giga pixel resolution.

Table 1: Simulation Parameters

Number of task	10
Number of virtual machines	7
Operating system	Linux
Architecture	64 bit
Encryption Data	Image type

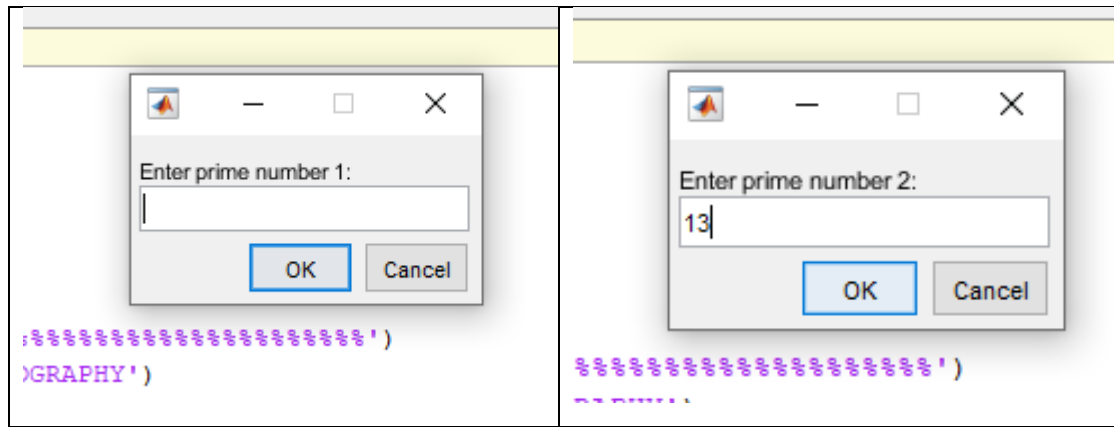


Figure 2: Enter prime Numbers

As shown in figure 2, the diffie helman algorithm is applied for the secure channel establishment. The prime number of entered for secure key generation

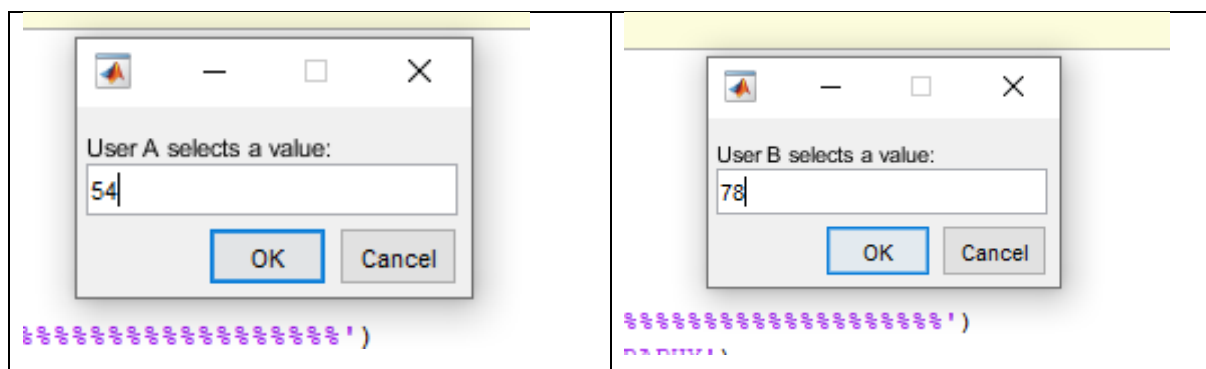


Figure 3: Enter Secret Keys

As shown in figure 3, the user A and B enter its secret keys for the secure key calculation.

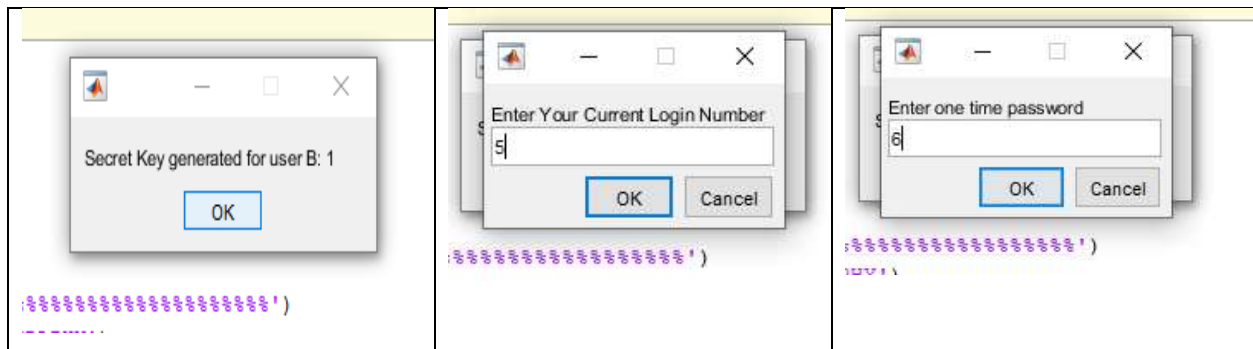
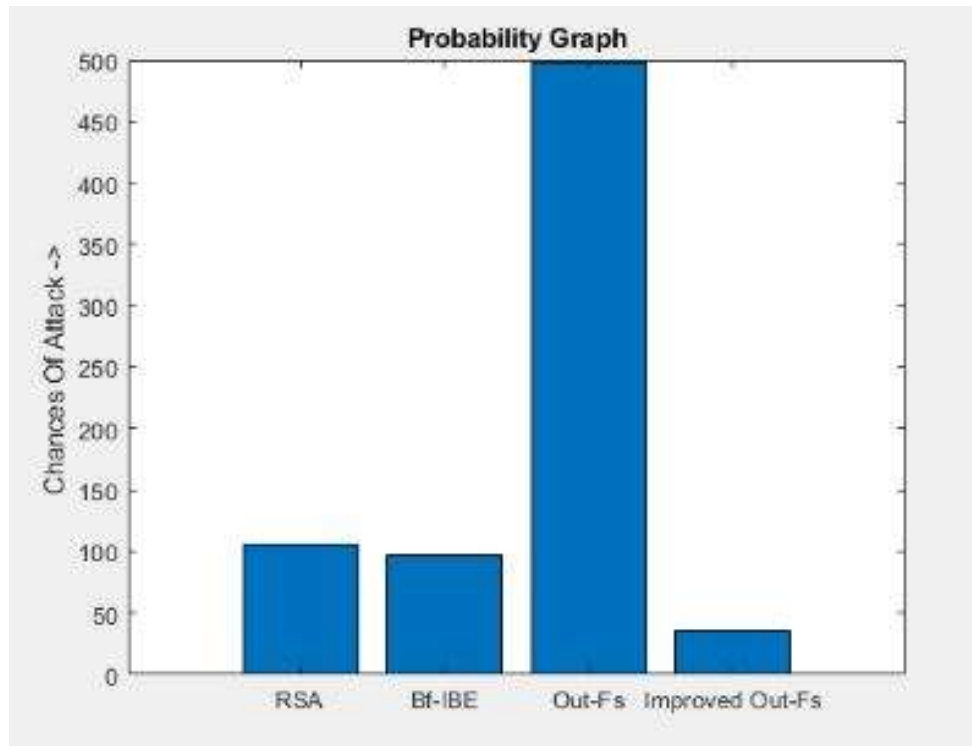


Figure 4: Generation of Keys

As shown in figure 4, the OTP is generated in this phase which is the combination of secret key and number of login times.

Table 1: Probability of Attacks

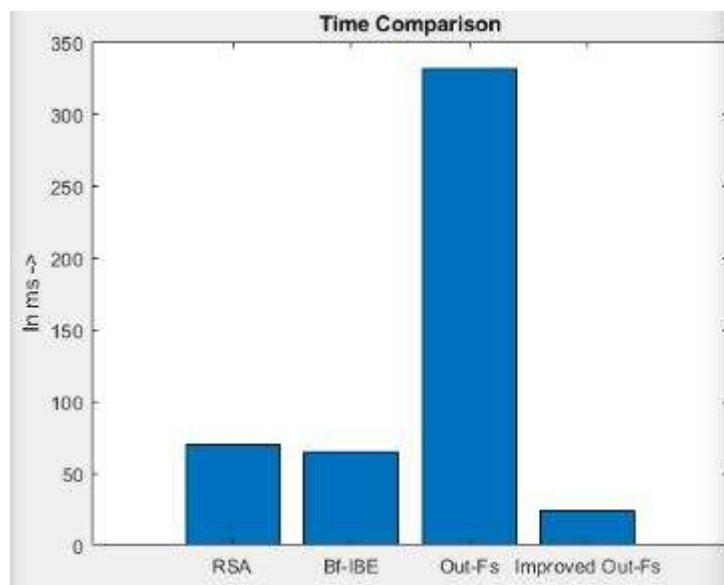
RSA	BF-IBE	Out-FS	Improved Out-FS
120	100	220	32


Figure 5: Attack Probability Analysis

As shown in figure 5, the attack probability of proposed technique is compared with Out-Fs, Bf-IBE and RSA. The Proposed technique has least chances of attack as compared to other techniques.

Table 2: Time Comparison

RSA	BF-IBE	Out-FS	Improved Out-FS
70	67	140	35


Figure 6: Time Analysis

As shown in figure 6, the Execution time of proposed technique is compared with Out-Fs, Bf-IBE and RSA. The Proposed technique has least execution time as compared to other techniques.

Table 3: Space Utilizations

RSA	BF-IBE	Out-FS	Improved Out-FS
3000	2800	2600	2500

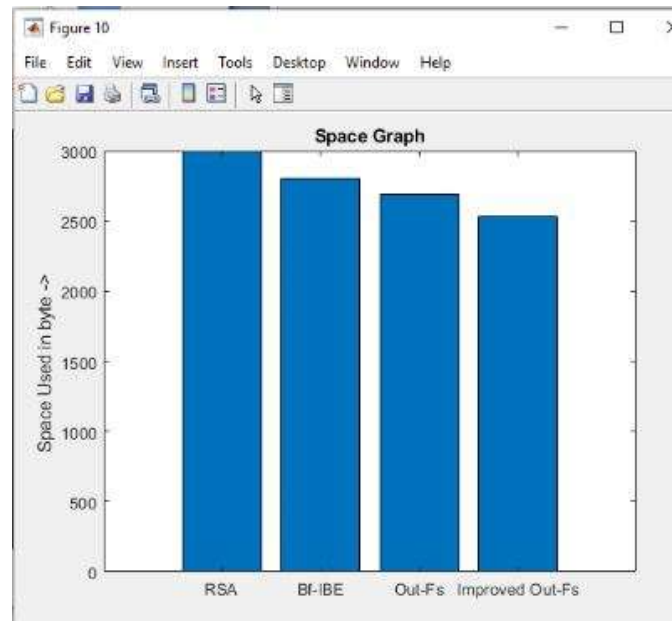


Figure 7: Space Utilization Analysis

As shown in figure 7, the space utilization of proposed technique is compared with Out-Fs, Bf-IBE and RSA. The Proposed technique has least space utilization as compared to other techniques.

5. CONCLUSION

The performance of 5G network is affected due to data breaches and security issues. Therefore, to provide security measures and privacy, the service providers focus on deploying cryptography methods, authentication approaches and virtualization. The control will no longer persist in the hand of user's id the service provider hosts the data and web applications. The encryption schemes are suggested for the secure authentication and certification in 5G. This work suggests a novel attribute based scheme will be proposed which will be less complex and more secure for the certificate distribution. The proposed method is the based on the differ-helman algorithm or the identity exchange. The homomorphic encryption (HE) approach is applied to encrypt the data. The proposed model is implemented on MATLAB and an analysis is conducted on results concerning energy, time and chances of attacks. It is analysed that proposed model performs well as compared to existing Identity-Based Encryption model for data security.

References

1. Chen, X. Ge and Q. Ni, "Coverage and handoff analysis of 5G fractal small cell networks", IEEE Transactions on Wireless Communications, vol. 18, no. 2, pp. 1263-1276, 2019.
2. H. Zhao and E. Al-Masri, "A user-centered handoff procedure in 5G cellular networks", Companion Proceedings of the Web Conference 2020 ser. WWW '20, pp. 107-108, 2020.
3. S. Basloom, N. Akkari and G. Aldabbagh, "Reducing handoff delay in SDN-based 5G networks using AP clustering", Procedia Computer Science, vol. 163, pp. 198-208, 2019.
4. P. Kulshreshtha and A. K. Garg, "Managing 5G networks - a review of fso challenges and solutions", 2020 11 th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-4, 2020.
5. G. V. Arevalo and R. Gaudino, "Optimal dimensioning of the 5G optical fronthaulings for providing ultra-high bit rates in small-cell micro-cell and femto-cell deployments", 2019 21st International Conference on Transparent Optical Networks (ICTON), pp. 1-4, 2019.
6. O. Tsopa, O. Dudka, A. Merzlikin and N. Ruzhentsev, "Estimation of the bandwidth of the communication channel of 5G networks based on small cells", 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), pp. 525-529, 2021.
7. P. Mukherjee et al., "A novel handoff algorithm for 5G", Computers and Devices for Communication, vol. 147, pp. 169-175, 2021.
8. M. F. Mustafa et al., "Handoff Management in Macro-Femto Cellular Networks" in Paving the Way for 5G Through the Convergence of Wireless Systems, IGI Global, pp. 227-249, 2019.
9. R. ThamaraiSelvi, S. Kevin Andrews, S. Radha Rammohan, Jayanthiladevi, and Nana Yaw Asabere, "Efficient Handoff Management in 5G Ultra Dense Networks Using Dynamic Beamforming Techniques," ICTACT Journal on Communication Technology, vol. 14, no. 2, June 2023.
10. V. Mishra, D. Das and N. N. Singh, "Novel Algorithm to Reduce Handover Failure Rate in 5G Networks," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 524-529,

- doi: 10.1109/5GWF49715.2020.9221410.
11. A. Ozhelvaci and M. Ma, "Secure and Efficient Vertical Handover Authentication for 5G HetNets," 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 2018, pp. 27-32, doi: 10.1109/ICICSP.2018.8549809.
 12. D. Wang, A. Qiu, Q. Zhou, S. Partani and H. D. Schotten, "Investigating the Impact of Variables on Handover Performance in 5G Ultra-Dense Networks," 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023, pp. 567-572, doi: 10.1109/EuCNC/6GSummit58263.2023.10188324.
 13. Y. Wei, R. P. Cabrera, C. -H. Lung and S. Ajila, "Pre-connect Handover Management for 5G Networks," 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 556-561, doi: 10.1109/FNWF55208.2022.00103.
 14. M. I. Goh, H. T. Yew, S. K. Chung, A. Kiring and A. I. Mbulwa, "AHP-TOPSIS Based Handover Algorithm with Distance Prediction for 5G Networks," 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA), Selangor, Malaysia, 2022, pp. 392-396, doi: 10.1109/CSPA55076.2022.9781889.
 15. M. Yoon, J. Park, T. Park, J. Seo, J. -K. Yun and K. Cho, "An Adaptive Handover Scheme to support UE with various movement speeds in 5G network," 2022 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Yeosu, Korea, Republic of, 2022, pp. 1-4, doi: 10.1109/ICCE-Asia57006.2022.9954717.
 16. A. Okaf, A. Saied and D. Qiu, "Analysis of Self-Blockage Impact on Handover Probability for User with Mobility in 5G Mm-Wave Cellular Network," 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1-5, doi: 10.1109/ISNCC52172.2021.9615850.
 17. K. Ouali, M. Kassar, T. M. Trang Nguyen, K. Sethom and B. Kervella, "An Efficient D2D Handover Management Scheme for SDN-based 5G networks," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2020, pp. 1-6, doi: 10.1109/CCNC46108.2020.9045534.
 18. L. Mei, J. Gou, Y. Cai, H. Cao, Y. Liu, "Realtime mobile bandwidth and handoff predictions in 4G/5G networks", Computer Networks, Volume 204, 2022, 108736, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2021.108736>.
 19. N. Zohar, "Beyond 5G: Reducing the handover rate for high mobility communications," in Journal of Communications and Networks, vol. 24, no. 2, pp. 154-165, April 2022, doi: 10.23919/JCN.2022.000001.
 20. V. K. Shaw and S. D. Roy, "Handoff Analysis in 5G Small Cell Network," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 655-659, doi: 10.1109/ICESC48915.2020.9155584.
 21. C. Roy and S. Misra, "Safe-Passé: Dynamic Handoff Scheme for Provisioning Safety-as-a-Service in 5G-Enabled Intelligent Transportation System," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5415-5425, Aug. 2021, doi: 10.1109/TITS.2021.3054694.
 22. N. Sharghivand, L. Mashayekhy, W. Ma and S. Dustdar, "Time-Constrained Service Handoff for Mobile Edge Computing in 5G," in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 2241-2253, 1 May-June 2023, doi: 10.1109/TSC.2022.3208783.
 23. A. I. Mbulwa, H. T. Yew, A. Chekima and J. A. Dargham, "Self-Optimization of Handover Control Parameters for 5G Wireless Networks and Beyond," in IEEE Access, vol. 12, pp. 6117-6135, 2024, doi: 10.1109/ACCESS.2023.3346039.
 24. Y. Zhang, R. H. Deng, E. Bertino and D. Zheng, "Robust and Universal Seamless Handover Authentication in 5G HetNets," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 858-874, 1 March-April 2021, doi: 10.1109/TDSC.2019.2927664.
 25. H. Zhang, W. Huang and Y. Liu, "Handover Probability Analysis of Anchor-Based Multi-Connectivity in 5G User-Centric Network," in IEEE Wireless Communications Letters, vol. 8, no. 2, pp. 396-399, April 2019, doi: 10.1109/LWC.2018.2873389.