A Multi-Layered Security Framework for High-Clearance Network Communication

Mr. Aditya Jaiswal
Department Of Computer Engineering
Shah And Anchor Kutchhi Engineering College
Mumbai, India
aditya.jaiswal15974@sakec.ac.in

Mr. Yash Rane
Department Of Information Technology
Shah And Anchor Kutchhi Engineering College
Mumbai, India
yash.rane_19@sakec.ac.in

Dr. Nilakshi Jain
Department Of Cybersecurity
Shah And Anchor Kutchhi Engineering College
Mumbai, India
nilakshi.jain@sakec.ac.in

***Abstract*—In the world of high-clearance organizations where the utmost security of communication is imperative, this research paper introduces a fortified network communication system designed to surmount the limitations of Hybrid Key Encryption (HKE) and VPN Tunnelling. By adding an additional layer of encryption through nested encryption techniques, augmenting security with a destructive defense agent based on rate limiters at decryption, and integrating a Machine Learning model into the communication channel for real-time threat prevention, this system strives to establish an unparalleled level of security. This research offers a promising avenue for safeguarding sensitive information and ensuring the confidentiality and integrity of communications among high-clearance entities in an era where data security is paramount.**

Keywords—Network Communication System, Hybrid Key Encryption, Nested Encryption, Destructive Defense Agent, Machine Learning.

I. INTRODUCTION

In an era of ever-present technological advancements and evolving cyber threats, high-clearance organizations have the burden of securing the communication channels that are used within their institution. In order to protect national interests and/or the many stakeholders involved in an organization, these agencies may put a remarkable amount of effort into guarding the secrecy of their most sensitive exchanges It is within this context that this research paper unveils a groundbreaking network communication system, meticulously engineered to overcome the constraints of conventional encryption methods and establish an impenetrable shield around their most sensitive data.

Hybrid Key Encryption (HKE) has long stood as a defender of data, its symmetrical and asymmetrical encryption paradigms beautifully molded together to ensure the ultimate confidentially, integrity and authenticity in the digital world. However, as the digital frontier continues to evolve, it has become increasingly apparent that even the most robust encryption techniques possess vulnerabilities that must be addressed to uphold the sanctity of communication.

This research aims at improving the current level of securing communication system by introducing a new kind of approach for communication security. The main agenda of the work is to provide a dual layer of encryption; by employing the further layer of encryption on the existing already encrypted data. So, in this way, the level of security will be increased to the maximum level and will be impossible for any unauthorized user to break that code and guard against the unauthenticated use of the data.

In addition to fortifying the encryption layers, the research paper establishes a promising new approach for blocking systems, based on rate limiters at the decryption phase of the transmission, which strikes at the heart of one of the most potent threats to cryptographic systems: brute force attacks.

Since this fortified communication channel can also be misused for communication of illicit activities, thus recognizing the importance of keeping individuals and society safe and secure, the project integrates the transforming power of machine Learning (ML). A trained ML model continuously resides on the communication channel and proactively monitors, scrutinizes and learns the pattern of traffic data moving remotely and in real time, also identifying anomalies, and initiating swift, preemptive measures to prevent illicit communication. In doing so, it shatters the traditional boundaries of security, propelling it into the realm of real-time threat prevention.

This research acts as a development guideline for improved communication channels, as it promises to redefine the very essence of communication security for high-clearance organizations.

II. LITERATURE REVIEW

Hybrid Key Encryption (HKE) which is a widely adopted cryptographic technique that combines the strengths of both symmetric and asymmetric encryption. The symmetric encryption component provides efficiency, while the asymmetric part offers enhanced security. However, as outlined in numerous studies [1], HKE is not immune to evolving threats. Quantum computing, for instance, poses a significant challenge to the security of asymmetric encryption systems. The paper [2] talks about vulnerabilities of traditional cryptographic algorithm generation techniques and introduces a groundbreaking algorithm for effective and efficient solution to the problem of mathematically computed cryptographic systems which includes logarithmic and integral factorization. When it comes to cryptographic security the major component is the computation using quantum computing. The paper [3] comprehensively elaborates about quantum computing and provides brief information about Noisy Intermediate-Scale Quantum and also challenges the security of cryptographic systems and concepts.

The processing of actual data to encrypted data using a cryptographic approach and creating a very strong and irreversible encryption algorithm is the major concern to ensure data security and confidentiality. This is shown in paper [4] where they talked about different ciphertext security

and choosing a robust technique using advanced and complex mathematics. This paper [5] mainly focuses on the role and effects of a strong encryption technique and how we can achieve data security. Constant evolving and upgrading from one stage to the next stage in a more secure and efficient manner is essential. Therefore, one cannot firmly stick to one technique and continuous betterment is necessary.

The paper [6] talks about the security of the SNOW 3G encryption algorithm and highlights the vulnerabilities of the same. As a result, the paper concludes that continuous research and enhancement of encryption methods is necessary. It also suggests the regular monitoring of the existing encryption methods to resolve any loopholes in the method. Whenever we talk about cryptography and data encryption, hashing, the only reason we are doing this to avoid and prevent any kind of attack over the network or on the data. Hence, the concept of nested encryption has gained attention in recent years as a means to bolster data security [4]. This technique involves encrypting already encrypted data, effectively creating multiple layers of protection. Researchers have explored the feasibility and advantages of nested encryption, highlighting its potential to thwart sophisticated attacks and augment data confidentiality. This approach aligns with our research's emphasis on adding an extra layer of encryption to HKE.

The paper [7] throws light on different attacks and also gives insightful details about the various cryptographic techniques. It talks about the practical and efficient design of such a secure cryptographic system. And now in the era of smart Machine Learning (ML) monitoring models we can integrate this self-learning ML models can be used as a dual-purpose tool for mainly threat detection and targeting adversaries. The paper [8] talks about the same ML models and their wide range of applications in security areas and threat detection. These ML models need to be trained and tested properly with a diverse variety of test cases to ensure that it work properly and is capable to give the desired and correct outcome as expected. The paper [8] spotlights how these ML models can be trained and also introduces the concept of deep learning to make sure that the privacy is not breached and the security, credibility and consistency of data is maintained.

Apart from that Brute force attacks, which involve exhaustive trial-and-error attempts to decrypt data, have posed a persistent threat to cryptographic systems. Prior studies have investigated various methods to mitigate these attacks, such as increasing key length and implementing rate limiting mechanisms [7]. Our research builds upon this knowledge by introducing a destructive defense module based on rate limiters during the decryption process to deter brute force attacks effectively.

The literature review underscores the evolving nature of cryptographic threats and the need for robust security measures to protect high-clearance organizations' sensitive communications. The research presented in this paper integrates nested encryption techniques and rate limiters for brute force attack deterrence, offering a comprehensive approach to address the limitations of HKE and provide the highest level of security for communication in this critical context.

III. Methodology

The communication security system outlined in this research represents a significant stride toward ensuring the confidentiality, integrity, and security of data within high-clearance organizations. By seamlessly integrating encryption, decryption, machine learning, and sophisticated attack mitigation techniques, this system stands as a beacon of innovation and resilience in the face of evolving cyber threats. As high-clearance organizations continue to navigate the digital landscape, this comprehensive security solution serves as a formidable shield against potential adversaries, offering peace of mind and unwavering data protection.

A. Sender's Terminal (Encryption Module)

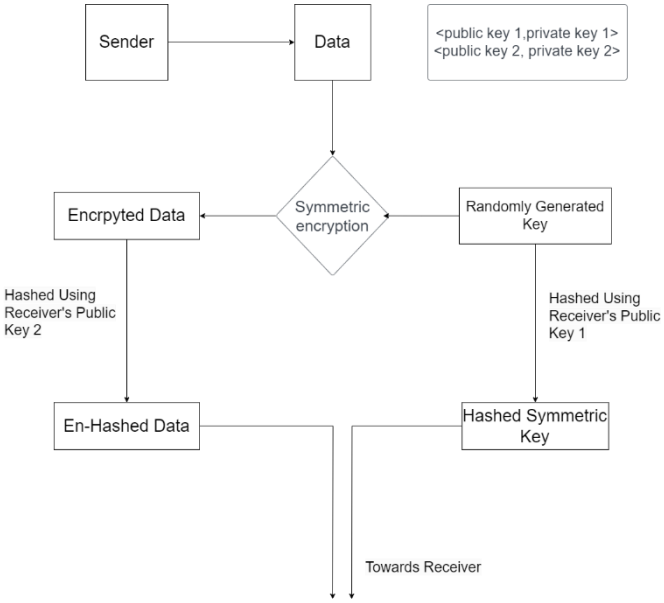

Fig. 1. Sender's Terminal System Flow Diagram

The initial step involves the sender's selection of the data to be communicated. This data remains in its original, unprocessed state and is not stored within the system. Subsequently, the selected data undergoes encryption using a high-complexity mathematical algorithm, similar to Symmetric Key Encryption. This encryption process is powered by a randomly generated key, ensuring that the data is transformed into a mathematically encrypted form. To reinforce security, the key employed for encrypting the data is hashed. This key hashing procedure involves the use of the receiver's public key 1. The outcome is that the key can only be decrypted by the intended receiver using the receiver's private key 1. Building upon the initial encryption, a double encryption layer is introduced. This involves encrypting the previously encrypted data, using the receiver's public key 2. This dual encryption process further fortifies the security of the data, since the data can only be decrypted using the receiver's private key 2. These meticulously orchestrated encryption steps form a robust security framework. They prioritize the confidentiality and integrity of the data while ensuring that only the intended receiver, armed with the respective public-private key pairs, can access and decrypt the data, providing a comprehensive solution for secure communication in high-clearance settings.

B. Receiver's Terminal (Decryption Module)

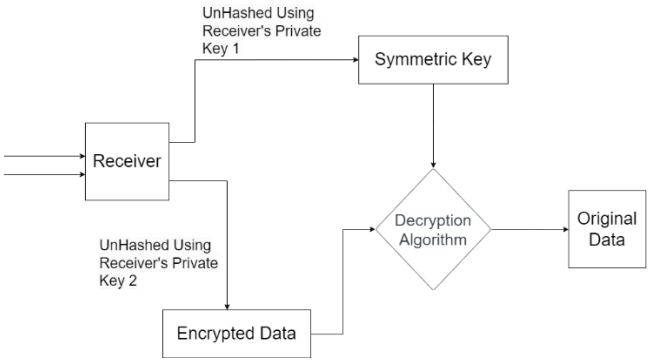

Fig. 2. Receiver's Terminal System Flow Diagram

Upon arrival at the receiver's end, the data is in a hashed format, ready for decryption and retrieval. The receiver initiates the decryption process by utilizing its private keys. The private key 2 is used to unhash the data packet, resulting in the retrieval of the initially encrypted data. The private key 1 is used to unhash the sender's symmetric key. Now that the actual symmetric key is available, it is used as an input for the decryption algorithm. The decryption algorithm employs the symmetric key to decrypt the encrypted data successfully. As a result of the decryption process, the encrypted data is transformed back into its original, readable form. The authorized receiver can now access and retrieve the actual data securely.

C. Self Learning ML Model

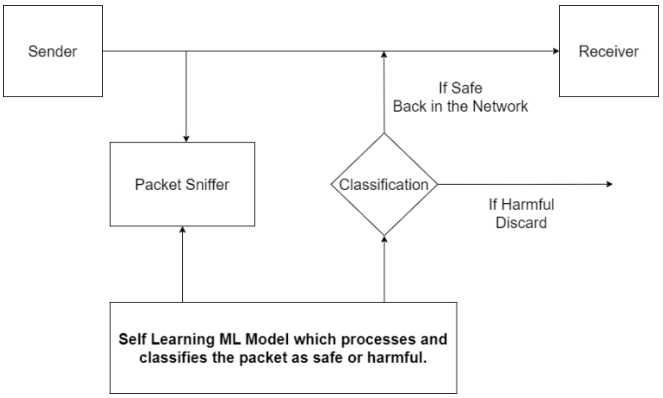

Fig. 3. Self-Learning ML Model's System Flow Diagram

Since this fortified communication channel can also be misused for communication of illicit activities, a self-learning ML model is deployed on the communication channel which proactively monitors, scrutinizes and learns the pattern of traffic data moving remotely and in real time, also identifying anomalies, and initiating swift, preemptive measures to prevent illicit communication. The ML model will function based on the following steps:

1) Gather a diverse dataset of network traffic packets, including both normal and potentially harmful data packets. Annotate or label the dataset to indicate which packets contain harmful or inappropriate content.

2) Extract relevant features from the network packets, such as packet size, source, destination, payload, and metadata. These features will be used for training the machine learning model.

3) Using models like convolutional neural networks (CNNs) or recurrent neural networks (RNNs) can be effective for developing the self learning functionality for packet classification.

4) Prepare the dataset by splitting it into training and testing sets. Normalize or preprocess the data to ensure it's suitable for training the model.

5) Train the selected machine learning model using the labeled dataset. The model should learn to classify packets as either "safe" or "harmful" based on the extracted features.

6) Integrate packet sniffing technology into the network infrastructure which will capture and inspect incoming data packets in real-time.

7) Implement a module that continuously analyzes incoming packets using the trained machine learning model. When a packet is received, it should be processed and classified as safe or harmful.

8) If a packet is classified as harmful or inappropriate, set up a mechanism to automatically discard or block that packet from being transmitted further. Ensure that the system logs the incident for auditing purposes.

D. Attack Mitigation

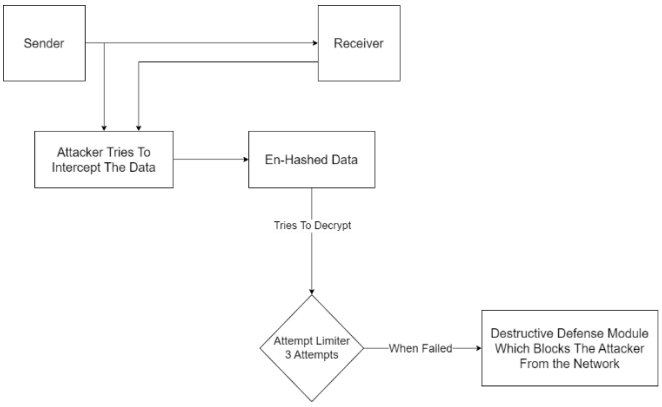

Fig. 4. Attack Mitigation's System Flow Diagram

Hackers, with their constantly evolving arsenal of techniques, pose a persistent threat to the integrity and confidentiality of data. These threats manifest in various forms, like Man In The Middle Attack, Spoofing, Brute Forcing and various other methods.

Now, a hacker attempts to gain access to the communication system, posing as an authorized user. In the event that the hacker successfully intercepts a data packet, they find themselves in possession of only the hashed data. The hacker faces the challenge of unhashing the content, a task deemed nearly impossible due to the robust hashing techniques employed, such as the SHA algorithm. Brute force approaches to unhash the content prove futile. To further deter the hacker's unhashing attempts, the system imposes strict constraints, allowing only three decryption attempts. These constraints are designed to thwart any brute force attacks on the hashed data. In the event that the hacker fails to successfully unhash and decrypt the packet within the limited number of allowed attempts, the communication system activates a Destructive Defense Model. The Destructive Defense Model, once activated, immediately blocks the hacker's access to the network. This action is taken to safeguard the safety and integrity of data packets. With the

hacker effectively blocked from further network access, the security system reinforces the principle that only the right and authorized users can access and decrypt the data packet, ensuring the confidentiality and security of transmitted data.

IV. Result

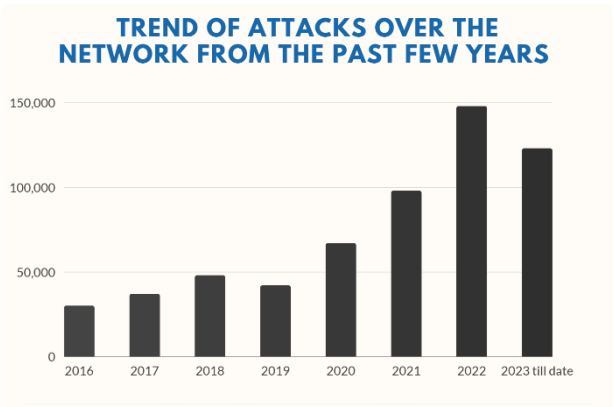

Fig. 5. Cyber Attack Trend Graph

In light of a recent survey conducted by Cisco, the findings as presented by Fig. 5. underscore a stark and concerning reality: that there is an ongoing and alarming surge in network attacks. Majorly, high-clearance organizations, dealing with sensitive data and national interests, are prime targets for these threats as there is a wealth of sensitive information, from classified documents to strategic plans. This escalating threat landscape has sent shockwaves through the digital realm, prompting a critical imperative for securing data and safeguarding its confidentiality. As organizations and individuals increasingly rely on network communication, the need to fortify data access, limiting it exclusively to authorized users, has never been more pronounced.

V. Future Scope

The research presented in this paper lays the foundation for a cutting-edge network communication system aimed at enhancing security within high-clearance organizations. While the current system represents a significant leap forward in safeguarding sensitive data, there are several avenues for future exploration and refinement that can further bolster its resilience and effectiveness. The future scope of this research encompasses a range of crucial aspects mentioned below.

A. Quantum Resistance

Future research could focus on making the proposed communication system quantum-resistant by developing encryption techniques that can withstand quantum attacks.

B. Advanced Machine Learning

Continuously improving and expanding the capabilities of the self-learning ML model is essential. Future developments might involve incorporating more advanced machine learning algorithms, such as deep reinforcement learning, to enhance the system's ability to detect and prevent threats.

C. Usability and Scalability

The proposed system should be tested for usability and scalability in real-world high-clearance organizations. Further research can explore how the system can be integrated seamlessly into existing communication infrastructure without causing disruptions.

D. Regulatory Compliance

Assess the system's compliance with relevant data privacy and security regulations, such as GDPR, HIPAA, or government-specific requirements. Ensure that the system aligns with legal and compliance standards.

E. Continious Monitoring and Updates

Implement a robust system for continuous monitoring of the communication channel, including regular updates to encryption algorithms, threat models, and machine learning models to adapt to evolving threats.

VI. Conclusion

In conclusion, this research paper presents a comprehensive network communication system designed to address the evolving challenges of data security in high-clearance organizations. By introducing nested encryption, a self-learning machine learning model, and a destructive defense mechanism, this system offers a multi-layered approach to safeguarding sensitive information. Using this system, we can avoid tunnelling, eliminate the threats to VPN systems and most importantly, the data security triad principles are upheld throughout the communication.

References

[1] Hoffmann, Leah & Diffie, Whitfield & Hellman, Martin. (2016). Finding New Directions in Cryptography. Communications of the ACM. 59. 112-111. 10.1145/2911977.

[2] E. Giusto et al., "Quantum Computing Reliability: Problems, Tools, and Potential Solutions," 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S), Porto, Portugal, 2023, pp. 2-3, doi: 10.1109/DSN-S58398.2023.00015.

[3] M. J. Hossain Faruk, S. Tahora, M. Tasnim, H. Shahriar and N. Sakib, "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities," 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, 2022, pp. 1-8, doi: 10.1109/ICAIC53980.2022.9896970.

[4] Canetti, R., Halevi, S., Katz, J., & Lindell, Y. (2004). "Chosen-Ciphertext Security from Identity-Based Encryption." SIAM Journal on Computing, 34(1), 146-175 S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[5] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," 2021 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 2021, pp. 616-622, doi: 10.1109/CDS52072.2021.00111.

[6] Mendel, F., Rechberger, C., & Schläffer, M. (2017). "On the (In) Security of SNOW 3G." Advances in Cryptology – CRYPTO 2017, 299-318.

[7] S. Sharma, A. Burtsev and S. Mehrotra, "Advances in Cryptography and Secure Hardware for Data Outsourcing," 2020 IEEE 36th International Conference on Data Engineering (ICDE), Dallas, TX, USA, 2020, pp. 1798-1801, doi: 10.1109/ICDE48307.2020.00173.

[8] N. Baracaldo and A. Oprea, "Machine Learning Security and Privacy," in IEEE Security & Privacy, vol. 20, no. 5, pp. 11-13, Sept.-Oct. 2022, doi: 10.1109/MSEC.2022.3188190.

[9] Bhattacharyya, S., Kalita, J. K., & Karforma, S. (2019). "Deep learning for anomaly detection: A survey." arXiv preprint arXiv:1901.03407.

[10] Dworkin, M. J. (2007). "Recommendation for Block Cipher Modes of Operation: Methods and Techniques." National Institute of Standards and Technology (NIST).

[11] Ding, J., Ge, L., & Xu, C. Z. (2017). "A survey on post-quantum cryptography." Frontiers of Computer Science, 11(3), 423-468.