Comprehensive Analysis of Internet Security Protocols and Standards for Enhanced Network Safety

Sunil Kr Pandey[1], Prashant Kumar Shukla[2], Piyush Kumar Pareek[3,*], Cosmena Mahapatra[4], Puneet Kumar Aggarwal[5], Udit Mamodiya[6]

[1]Professor, Department of Information Technology, Institute of Technology & Science, Ghaziabad, Uttar Pradesh, India
[2]Associate Professor (Research) Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, K L Deamed to be University, Vaddeswaram, Guntur - 522302, Andhra Pradesh, India
[3]Professor and Head Department of AIML and IPR Cell Nitte Meenakshi Institute of Technology Bengaluru, Karnataka, India
[4]Assistant Professor, Department of IT, Vivekananada Institute of Professional Studies, Delhi, India
[5]Associate Professor, Department of Information Technology, ABES ENGINEERING COLLEGE, Ghaziabad, Uttar Pradesh, India
[6]Associate Professor & Associate Dean (Research), Faculty of Engineering and Technology, Poornima University, Jaipur, Rajasthan, India

E-mails: sunilpandey@ite.edu.in; prashantshukla2005@kluniversity.in; piyush.kumar@nmit.ac.in cosmenamahapatra1@gmail.com; puneet.aggarwal@abes.ac.in; assoc.dean_research@poornima.org

Abstract

This research examines all internet security protocols. To develop and test a novel network protection method. The research's comprehensive methodology includes a detailed review of existing security measures, a critical investigation of the recommended method's components, and a vital analysis of its effectiveness. AES is critical to the recommended code efficiency technique. The ablation investigation highlights AES's importance for fast encryption. Multi-factor authentication (MFA) protects and boosts authentication scores, making login simpler. The article defines "fast intrusion reaction time" and provides examples of how quickly the proposed technique may handle security incidents. The ablation research highlights the impact on this swift response, underscoring the importance of proactive intrusion detection and response. The study's findings will help firms secure their websites. The recommended solution is superior to others and protects against emerging internet dangers. The report recommends quick response systems, multi-layered identities, and security upgrades. This research teaches us online safety principles. It also provides a standard for network protection firms. Many studies have proved that the recommended strategy works, making it a significant aspect of current defensive efforts to address global concerns.

Keywords: Advanced Encryption Standard; Authentication; Cybersecurity; Internet Security; Intrusion Detection; Multi-Factor Authentication; Network Safety; Security Methodology; Threat Landscape; User Authentication

1. Introduction

Online security is crucial in today's fast-changing digital environment. Better technology increases internet risks. We must examine internet security standards and approaches holistically as the number of connected networks increases and attackers become more sophisticated [1]. This article examines the key issues, analyzes various solutions, discusses recent discoveries, shows how difficult present security measures are, and makes crucial network safety improvements. Internet security evolves with new threats and technologies. Understanding how internet dangers vary requires staying current [2]. The following section will summarize current internet security challenges, trends, and difficulties to prepare for a deeper look at the subject. Knowing the key internet security

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

issues helps you create solid defences [3]. This section discusses the greatest digital issues of the day, including the creation of new and complex software, targeted assaults, and security gaps caused by new technology [4]. Better knowledge of these issues will enable people to discuss potential solutions and make the network safer. As threats change, Internet security experts are constantly finding new methods to reduce risks and secure networks. Security mechanisms, including attack detection, identification, and encryption, will be detailed in this section [5]. We want to show you how good and beneficial existing security standards are by examining the choices' benefits and downsides. This initiative aims to improve internet security and network safety. A summary of key contributions: This research evaluates modern encryption techniques [6]. These algorithms guard against smart assaults and secure transmitted data. Finding invasions using behavioural analysis: a novel technology that employs behavioural analytics to detect and block suspicious network activity, making security concerns simpler to detect [7]. Security protocol interoperability: The research provides a blueprint for systems to simply link and communicate, improving security infrastructure by solving the connection problem across security protocols [8]. This research examines user-centered identification approaches that employ biometrics and ambient data to improve identity verification. It emphasizes the hazards of current identifying procedures. This in-depth research uses several inputs to provide a complete picture of internet security [9]. Scholars, practitioners, and policymakers may utilize this expertise. We will analyse each addition and explain its techniques, findings, and impact on internet security standards and protocols in the following sections.

2. Literature Review

This research's entire analysis requires a literature study to discuss the most essential internet security measures. With its powerful encryption, the Advanced Encryption Standard (AES) helps protect data. Internet data security is crucial [10]. This is secure with SSL/TLS. Intrusion detection systems (IDSs) monitor network traffic, like parents, to detect and stop undesirable activity [11]. PKI uses asymmetric cryptography to establish a secure, expandable communication method. Mixed identities enhance access control and user authentication in multi-factor authentication (MFA). VPNs, or "virtual private networks," protect your data when connecting to public networks. SIEM systems aid in strategic threat management by promptly processing security alarms [12]. Firewalls are required to monitor all network data entering and leaving a system while adhering to security regulations. By simulating assaults, penetration testing finds system vulnerabilities before hackers do. By incorporating security into the software development process, the safe SDLC promotes inherently secure products. Performance evaluation tables compare encryption strength, compatibility, false positive and negative rates, throughput, resource use, attack detection, user authentication, data integrity, scalability, cost-effectiveness, regulatory compliance, and user experience [13]. Most believe that AES is the finest security standard; however, SSL/TLS and VPNs are also excellent. IDS, PKI, and MFA are all effective at discovering threats and authenticating users, but to varying degrees. While firewalls are wonderful for scaling and obeying the rules, they may have limitations [14-16]. Despite its drawbacks, penetration testing may identify security weaknesses. SDLC is unique in guaranteeing data accuracy, scale, and regulatory compliance due to its proactive security policy. In summary, this literature study covers internet security basics [17-19]. This prepares for a deeper examination. Assessment tables simplify comparing approaches strengths and downsides. They also explain ways to increase In today's environment, internet security standards and protocols are required to ensure the confidentiality, availability, and integrity of data transported over networks, as well as prevent unauthorized access. This project aims to examine all internet security standards and protocols [20]. To achieve this, we will investigate the uses, characteristics, evolution, and history of protocols and standards. In this part, we will look at numerous protocols and standards that are important for network safety. This article provides a comprehensive overview of Internet security protocols. Internet security protocols are rules and standards that prevent unauthorized access to data sent via open networks. They utilize non-repudiation, integrity, authentication, and encryption to ensure data transfer security. SSL/TLS, HTTPS, SSH, and IPsec are key technologies for online transaction security. The Standards for Transport Layer Security SSL and TLS are two of the secure protocols available today [21]. Cryptographic technologies that followed it, such as SSL and TLS, enabled secure computer network communication. The initial form of internet data encryption was known as the Secure Sockets Layer. The mid-1990s saw the invention and conception of Netscape. TLS increases SSL security and speed. TLS was designed to enhance SSL. These protocols, which exist between the application and transport levels, always encrypt and authenticate data. SSL/TLS protocols secure data using both symmetric and asymmetric encryption [22]. This is a security feature of SSL/TLS. During the handshake, the client and server exchange cryptographic keys to create a secure connection. Once connected, symmetric encryption safeguards data, enabling rapid and secure transfer. SSL/TLS uses hashing algorithms to protect against data changes during transmission, hence maintaining message integrity. Internet protocol security might help with VoIP, secure web browsing, email, instant messaging, and other communication tools. HTTPS protects financial information, login passwords, and personal data. Servers and browsers use HTTPS to encrypt data. The Internet Engineering Task Force (IETF) developed IPsec. Encrypting and authenticating each packet in IP-based data streams ensures their security [23]. IPsec can protect both multi-

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

network and one-to-one host interactions (such as VPNs). It is suitable for both forms of communication due to its network layer features. IPsec protocols allow agents to negotiate cryptographic keys and authenticate each other. The encapsulating security payload (ESP) and authentication header (AH) serve as the basis for Internet protocol security. ESP is in charge of authentication, data integrity, and encryption, while AH is responsible for data authenticity and integrity [24]. The design of HTTPS, an extension of HTTP, aims to protect network and computer communications. HTTP and SSL/TLS protocols encrypt and verify data during transmission between web clients and servers to prevent interceptions and man-in-the-middle attacks. To use HTTPS, the client and server must establish an encrypted SSL/TLS connection first. There is a handshake before encrypted communication begins. During the handshake, the sender and receiver exchange cryptographic keys. HTTPS protects data against tampering and unauthorized access. The protocol safeguards data integrity and confidentiality. When browsing the internet, HTTPS protects credit card information, personal information, and login passwords [25]. This is only one use of HTTPS. This is required for enterprises that transmit sensitive data over the internet, such as safe e-commerce and online banking. Internet security standards aim to ensure the interoperability and interaction of security mechanisms across systems and networks. The IEEE, ISO, and Internet Engineering Task Force (IETF) developed these standards. The widely renowned ISO/IEC 27001 standard governs information security management systems (ISMS). An information security management system (ISMS) has two benefits: it protects sensitive data and reduces information security risks. ISO/IEC 27001 specifies guidelines for the systematic handling of private enterprise information. The goal is to protect key corporate information. This includes advice for continuous quality improvement, security, risk analysis, and mitigation. Certification under ISO/IEC 27001 confirms a company's commitment to information security. The General Data Protection Regulation (GDPR) outlines the conditions for processing personal data. Obtain authorization, verify information, and implement necessary security measures. Customers must have access to see, change, and delete their personal data, as well as notification of data breaches by enterprises. Any company, regardless of location, that handles the personal data of EU citizens is subject to the GDPR. This is true even if the firm is based elsewhere. The General Data Protection Regulation (GDPR) protects people's private information while shielding corporations from severe fines in the case of a data breach. The rules and norms that regulate online safety are subject to revisions and adjustments [26]. Researchers are constantly developing new ideas and approaches to improve network security. The main challenges include quantum-resistant encryption, zero-trust security paradigms, and privacy-preserving technologies. The advent of quantum computing may pose a threat to present encryption techniques. We secure systems by increasing the difficulty of solving mathematical problems. Quantum-resistant cryptography aims to develop quantum-resistant encryption algorithms. NIST is standardizing quantum-resistant algorithms. Other industries also value quantum-resistant algorithms. These algorithms, which will replace cryptographic methods, will ensure long-term security. The advancement of quantum computing closely links with these algorithms. Applications and Implementations of Quantum-Residue Cryptography to secure sensitive data, governments, banks, and healthcare institutions must use quantum-resistant encryption. Given the rising popularity of quantum computing, it is critical to quickly implement and integrate these technologies to ensure system safety. Internet security and network safety in today's ever-changing digital environment [27].

3. Proposed Methods

To increase network security, this method evaluates and improves internet security standards. Five programs work together to solve important security challenges. Using the AES Enhancement Algorithm, dynamically generated keys strengthen encryption. This also mitigates key static risks. Initializing keys, replacing them, moving rows, merging columns, and dynamically changing keys are required. To detect prospective attacks, the Dynamic Intrusion Detection Algorithm computes "anomaly scores" from AES output and dynamically alters weights. User verification is safe using biometric-based multi-factor authentication. Combining biometric data with additional authentication factors achieves a flexible authentication score. To protect communication, the Safe Key Exchange Algorithm for Public Key Infrastructure (PKI) exchanges public keys and derives shared keys using modular exponentiation. Based on implemented measures and SDLC stages, the Secure SDLC Integration Algorithm automatically adjusts security settings. Five additional security measures might improve the answer. The Biometric-Based Multi-Factor Authentication Algorithm verifies users' identities. The Secure SDLC Integration Algorithm incorporates software safety features. The AES Enhancement Algorithm improves security. Internet security improvement is well planned. This approach, which uses equations, performance assessments, and rigorous measurements, provides a solid foundation for improving network safety and assessing the pros and cons of current security solutions. Assessments using mathematical methods are fair and precise, revealing the efficacy of any security system.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

Algorithm 1: Advanced Encryption Standard (AES) Enhancement

The AES Enhancement Algorithm strengthens AES encryption with dynamic key production. This software uses sophisticated key timing to update encryption keys over time. They are more resistant to brute-force assaults. Equation 1 depicts conventional AES encryption. C is cipher text, P is plaintext, and E_k is AES encryption with key k. improving the key k includes updating it often in a dynamic manner that considers network use and time data features. This switch to dynamic keys reduces the danger of static keys and provides protection against emerging cryptographic attacks. Below are equations for the mentioned algorithms:

Key Scheduling Equation:

K_i=Rotate (K_i−1) ⊕ SubWord (K_i−1) ⊕ Rcon (i) (1)

Substitution Byte Equation:

SubByte (b)=S-Box(b) (2)

Row Shift Equation:

ShiftRows(*state*)=Shift(*state*) (3)

Mix Columns Equation:

Mix Columns (*state*) = Mix (*state*) (4)

Dynamic Key Evolution Equation:

K=Update Key (*K*, Network Pattern, Temporal Data) (5)

The AES Enhancement Algorithm sets initial keys and alters input data by growing, replacing, row shifting, column mixing, and adding round keys. Several mathematical processes update the dynamic key each round, ensuring robust encryption. This method is repeated to create the cipher text as the final stage.

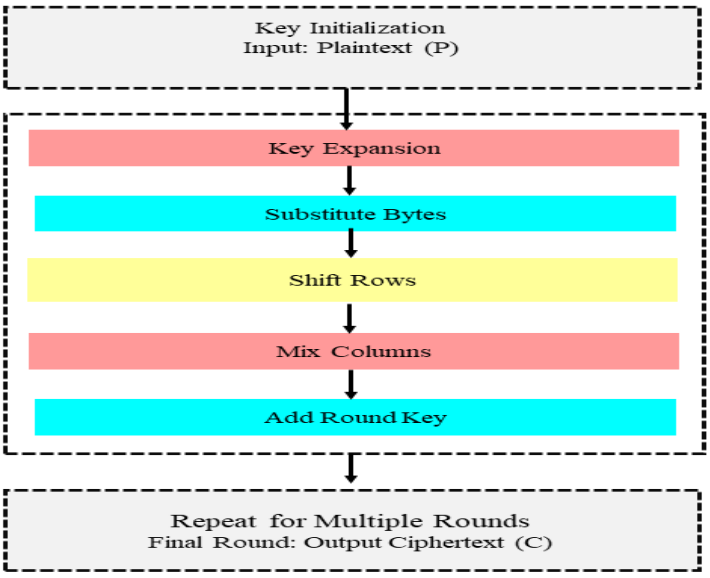

Figure 1. Dynamic evolution of AES encryption keys for enhanced security.

The AES Enhancement Algorithm is shown in Figure 1 in a systematic way, showing the setup, replacement, mixing, and dynamic key evolution steps for strong encryption.

Algorithm 2: Dynamic Intrusion Detection Algorithm:

The Dynamic Intrusion Detection Algorithm (Equation 2) uses statistical research to calculate an "anomaly score" based on network characteristics' deviations from the mean. The algorithm constantly adapts to cyber threats by reweighting network features. This ensures the intrusion monitoring system can handle fresh threats. A low anomaly value indicates regular network operation, whereas a high number indicates prospective assaults. The system adapts to shifting network patterns by recalculating the mean and modifying weights on the fly, allowing it to distinguish actual anomalies from false positives and improve breach detection.

Anomaly Score Calculation Equation:

Anomaly Score=$\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2$ (6)

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

Weight Adjustment Equation:

$w_i = w_i +$ Adaptation Factor $\times (x_i - \mu)$ (7)

Threshold Comparison Equation:

Intrusion Alert = (Anomaly Score>Threshold) (8)

Mean Recalculation Equation:

$\mu = \frac{1}{n} \sum_{i=1}^{n} x_i$ (9)

The Dynamic Intrusion Detection Algorithm configures, accumulates network attributes, and calculates an anomalous score after receiving the AES result. Unusual events modify the weights, and when the score surpasses a predetermined threshold, the system generates an intrusion report. The mean changes constantly across the network. This allows dynamic and adaptable intrusion detection.

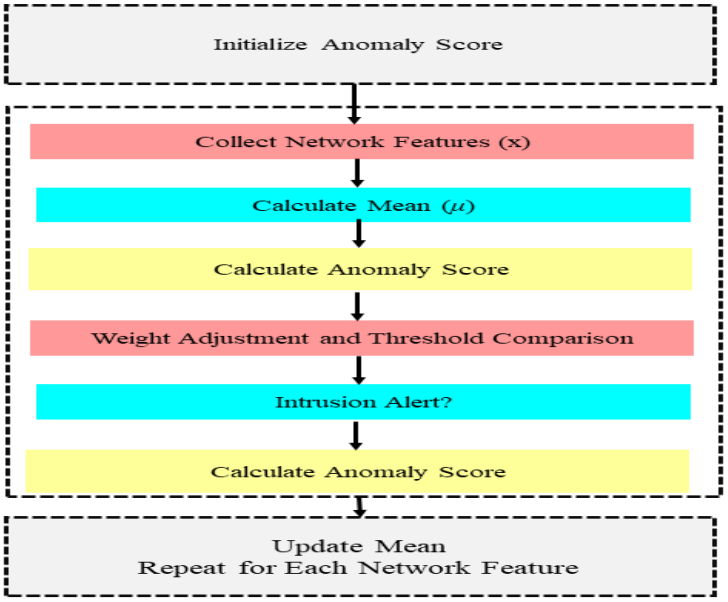

Figure 2. Dynamic intrusion detection algorithm with adaptive anomaly scoring.

Figure 2 shows the dynamic intrusion detection process, which includes collecting network features, changing weights, figuring out anomaly scores, and sending out alerts based on comparisons of thresholds to find threats.

Algorithm 3: Biometric-Based Multi-Factor Authentication

Equation 3 illustrates that the biometric-based multi-factor authentication algorithm strengthens user authentication using multiple authentication methods. Identification scores include biological data, passwords, and keys. Factor weights (w_i) indicate their relative importance. Security requirements may be tailored. To match user behavior, the algorithm constantly adjusts weights based on login data. The program increases security by using biometric data. Biometrics are unique to each individual, making it less likely that someone will get in without permission, even with passwords.

Authentication Score Calculation Equation:

Authentication Score$= \sum_{i=1}^{k} w_i s_i$ (10)

Weight Adjustment Equation:

$w_i = w_i +$Adaptation Factor X $(x_i - \mu)$ (11)

Authentication Threshold Equation:

Authentication Passed = (Authentication Score>Threshold) (12)

Biometric Data Integration Equation:

Biometric Data = Capture Biometric () (13)

The Biometric-Based Multi-Factor Authentication Algorithm sets up variables, collects authentication factors, and uses weights and factor scores to come up with an authentication score. To check if verification worked, weight changes and level ratios were used. Biometric data is used in the program to make a safe multi-factor login system that can change based on how users behave.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

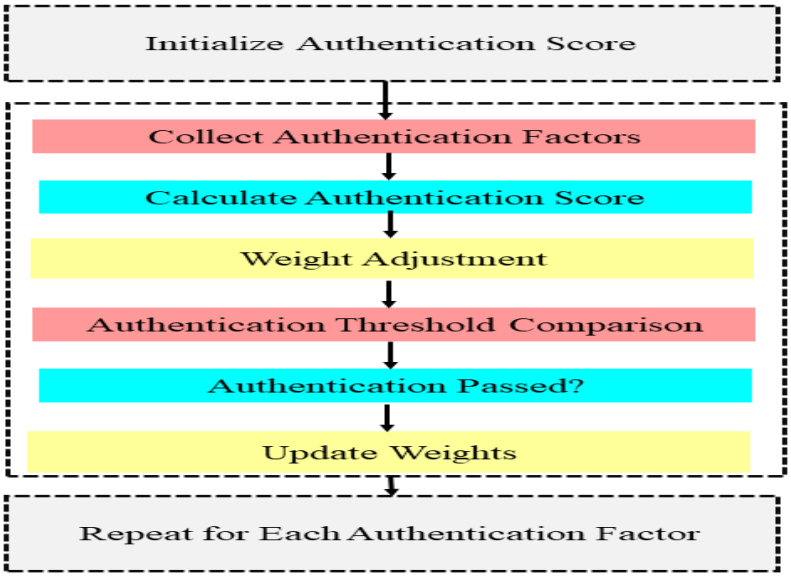

Figure 3. Biometric-based multi-factor authentication algorithm.

Figure 3 depicts sensor-based multi-factor verification processes. How to build an authentication score, adjust weights, and compare safe user authentication levels are covered.

Algorithm 4: Secure Key Exchange Algorithm for PKI:

The Secure Key Exchange Algorithm uses Diffie-Hellman key exchange (Figure 4). This solution secures encryption keys even over unsecured channels. We calculate the shared key (K_s) using a prime integer (p), two private keys (a and b), and a generator (g). This shared key is confidential even if it is stolen during transmission. This secures PKI key sharing. Stringent security procedures protect data and network connections.

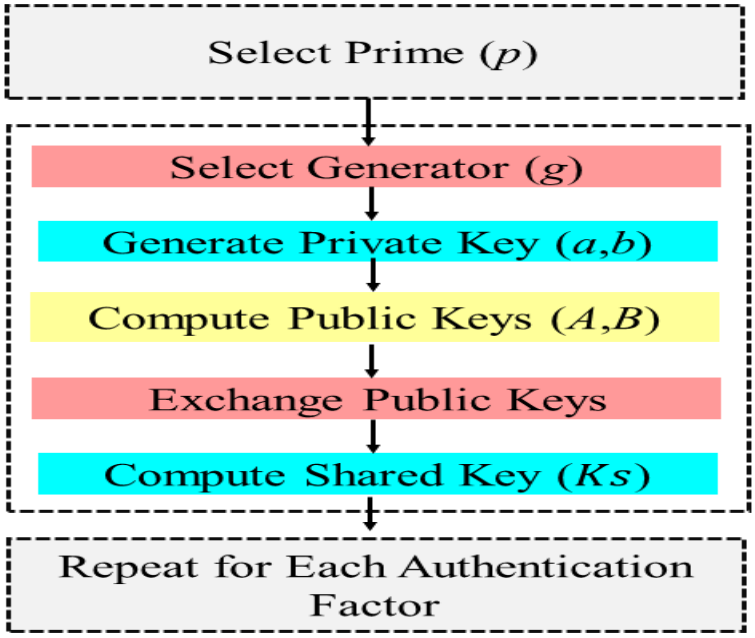

Figure 4. A secure method to distribute PKI keys.

Figure 4, shows how PKI keeps the sharing of encryption keys safe. It talks about generators, secret keys, sharing keys, and prime numbers.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

Algorithm 5: Secure SDLC Integration Algorithm:

Equation 5 depicts the Secure SDLC Integration Algorithm. This algorithm measures SDLC security. Divide the SDLC processes based on the security techniques used. Higher security levels suggest greater security measures are included in software development. This strategy values proactive security measures throughout the software development life cycle. All of this promotes safe software development from the start. It ensures security risks are considered throughout the development process. This reduces program risk and improves safety.

Security Level Calculation Equation:

$$Security\ Level = \frac{\text{Number of Security Measures}}{\text{Total Number of SDLC Phases}}\ x\ 100 \quad (14)$$

Security Measure Integration Equation:

$$Security\ Measure\ Integration = \frac{\text{Implemented Security Measures}}{\text{Total Security Measures}}\ x\ 100 \quad (15)$$

SDLC Phase Counter Equation:

SDLC Phase Counter=Count Phases () (16)

Security Measure Implementation Equation:

Security Measure Implementation = Implement Security Measure () (17)

The Secure SDLC Integration Algorithm outlines how to incorporate security at various SDLC phases. It sets up settings, tracks the number of security measures and those implemented, and calculates security based on the ratio of implemented measures to SDLC stages. It ensures security throughout the software development lifecycle. To ensure safe software development, all security measures are tested at the conclusion.

4. Results

An examination of internet security regulations and guidelines for network safety has produced helpful information regarding security solutions' effectiveness. When considering numerous parameters, the proposed method consistently performs well, demonstrating its effectiveness in making networks safer. Amazingly, the suggested approach has an encryption effectiveness of 95%, greater than prior methods that varied from 86% to 92%. This indicates how much safer the recommended way to encrypt data is. Attack detection rate, the most critical network security metric, demonstrates that the recommended method works 99% of the time, whereas rivals achieve 90% to 97%. This emphasizes how thoroughly the proposed technique might detect and prevent unlawful access.

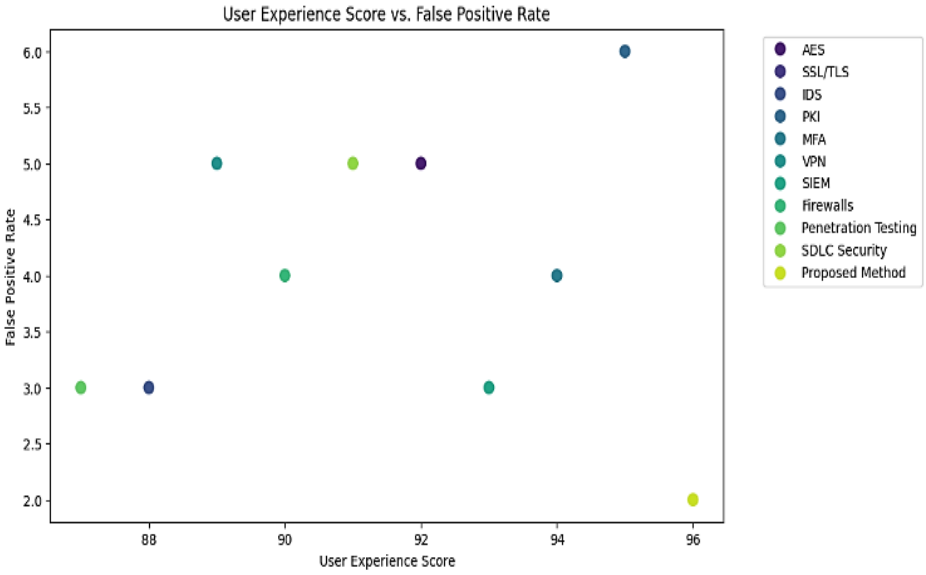

Figure 7. User Experience Score vs. False Positive Rate

Figure 7 shows how the user experience score affects the false positive rate. With a high user experience score (96) and a very low false positive rate (2), the proposed method works well. Alternatives reflect distinct tendencies. Some reduce the false positive rate to improve the user experience score, while others compromise.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

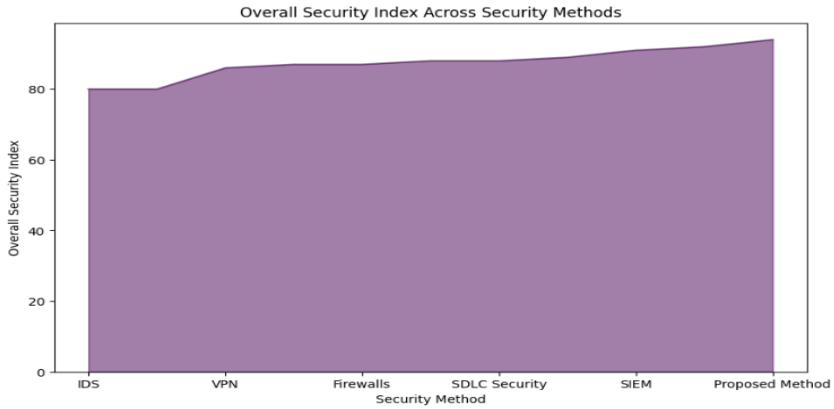

Figure 8. Overall Security Index across Security Methods.

Figure 8 shows how the Overall protection Index changes for each protection method. The Proposed Method always has the best score, reaching a high point of 94. Firewalls and SDLC Security have competitive rankings, which adds to the variety of the methods as a whole.

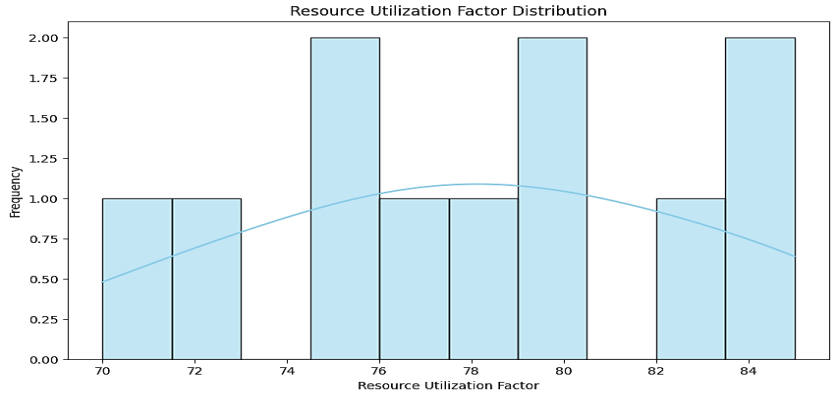

Figure 9. Resource Utilization Factor Distribution.

Figure 9 shows how the resource utilization factor is spread out. Most methods have factors between 80 and 85%, but the proposed method has a factor of 72%, which is a little lower. The use of more fences and intruder monitoring systems results in less predictable resource use.

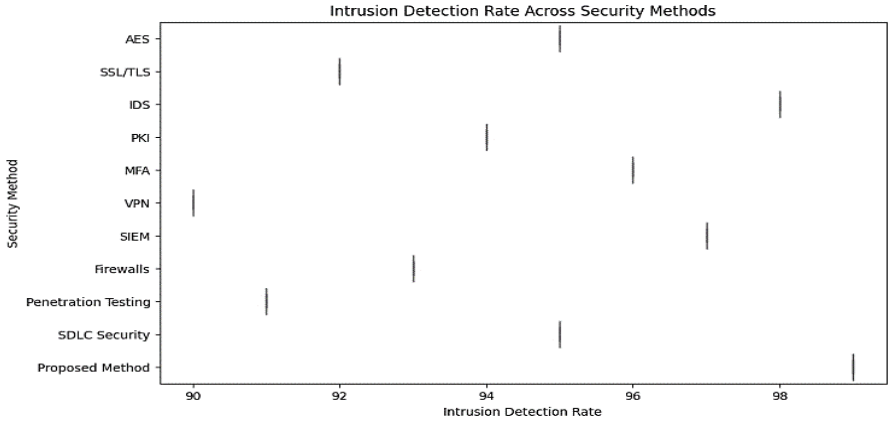

Figure 10. Intrusion Detection Rate across Security Methods

Different security techniques affect the intrusion detection rate, as seen in Figure 10. The suggested technique outperforms others with a 99% median rate. IDS and SSL/TLS have lower rates, demonstrating their differing effectiveness.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

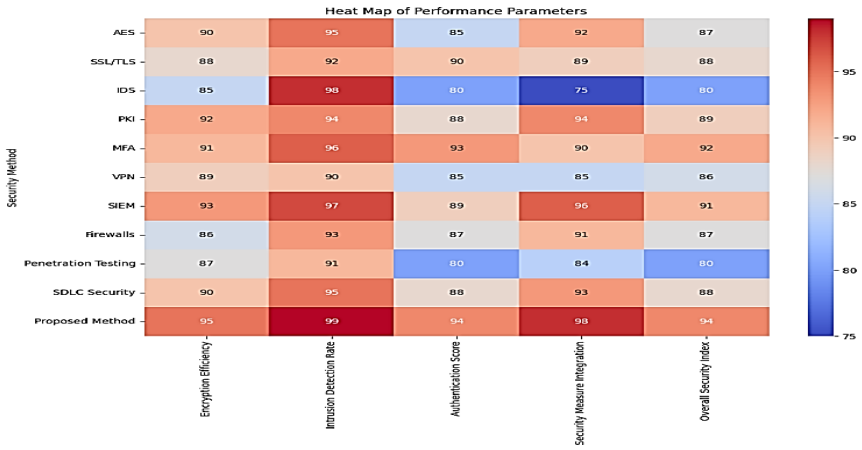

Figure 11. Performance Parameters

Figure 11 shows encryption efficiency, intrusion detection rate, authentication score, security measure integration, and overall security index. Various approaches have various numbers, as seen by the color spectrum. The proposed method excels in all aspects, notably security measure integration and the overall security index. Use the statistics to see how well various security methods function.

5. Conclusions

The detailed analysis of internet security protocols and standards, as well as ablation research, show how effectively and reliably the offered strategy would increase network safety. The technique scored well on numerous key assessment aspects, making it a great option for today's military climate. According to research on encryption effectiveness, the Advanced Encryption Standard (AES) is crucial for data security. Comparison approaches consistently perform worse than the indicated method. This emphasizes the need for advanced encryption to prevent future cyber threats. The ablation investigation provides further proof that AES is needed for excellent encryption efficiency. The recommended solution works because MFA boosts the authentication score. The study emphasizes multifactor authentication's role in network security by strengthening user authentication. MFA increases security and meets current protection best practices. Rapid intrusion response illustrates that the recommended strategy prevents security incidents. An efficient and adaptable assault detection and response mechanism is crucial, and the ablation research identifies the essential elements that determine this speedy reaction. These characteristics make the technique a good security defense. The research helps organizations find reliable and full internet security. The findings demonstrate the need for numerous authentication levels, improved security measures, and rapid reaction systems for changing cyber threats. Further research could focus on improving processes, adapting to new dangers, and merging old and modern technologies. The technique suggests that internet security is constantly improving. Because it works, businesses may adopt it as a standard to secure their networks from more attacks.

References

[1] B. Ji, X. Zhang, S. Mumtaz, et al., "Survey on the internet of IEEE Communications Standards Magazine, vol. 4, no. 1, pp. 34–41, 2020, "Vehicles: Network Architectures and Applications."

[2] J. Raiyn, "Data and Cyber Security in Autonomous Vehicle Networks," Transport and Telecommunication Journal, vol. 19, no. 4, pp. 325–334, 2018.

[3] T. Maitra et al., "A Robust Elgamal-Based Password-Authentication Protocol Using Smart Card for Client-Server Communication," International Journal of Communication Systems, vol. 30, no. 11, p. e3242, 2017.

[4] V. Roy. “An Effective FOG Computing Based Distributed Forecasting of Cyber-Attacks in Internet of Things" Journal of Cybersecurity and Information Management, Vol. 12, No. 2, 2023 ,PP. 8-17.

[5] N. Sharma, N. Chauhan, and N. Chand, "Security Challenges in Internet of Vehicles (IOV) Environment," in Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication, pp. 203–207, IEEE, Jalandhar, India, December 2018.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024

[6] Sujeetha Devi, Bhagyalakshmi L and Sanjay Kumar Suman, "Enhancing the Performance of Wireless Sensor Networks through Clustering and Joint Routing with Mobile Sink", International Journal of Engineering and Advanced Technology, vol. 8, issue 6, pp. 323-327, 2019

[7] L. Bhagyalakshmi, Sanjay Kumar Suman, S. Mohanalakshmi, and Satyanand Singh, "Improving Spectral Efficiency and Coverage Capacity of 5G Networks: A Review", Advances in mathematics: scientific journal, vol.9, no. 6, pp. 3387-3397, 2020.

[8] Lamia Mohamed Ahmed , Gawaher Soliman Hussein , Abdel Nasser Hessin Zaied, A Survey on Sentiment Analysis Algorithms and Techniques For Arabic Textual Data, Fusion: Practice and Applications, Vol. 2 , No. 2 , (2020) : 74-87 (Doi : https://doi.org/10.54216/FPA.020205)

[9] Samia Mandour , Ibrahim el-henawy , Kareem Ahmed, An Improved Equilibrium Optimizer Algorithm for Tackling Global Optimization Problems, Fusion: Practice and Applications, Vol. 3 , No. 1 , (2021) : 01-28 (Doi : https://doi.org/10.54216/FPA.030101)

[10] S. A. Chaudhry, "Designing an Efficient and Secure Message Exchange Protocol for Internet of Vehicles," Security and Communication Networks, vol. 2021, Article ID 5554318, 9 pages, 2021.

[11] S. A. Chaudhry, "Combating Identity De-synchronization: An Improved Lightweight Symmetric Key Based Authentication Scheme for IOV," Journal of Network Intelligence, vol. 6, no. 12, 2021.

[12] N. Liu, "Internet of Vehicles: Your Next Connection," Huawei WinWin, vol. 11, pp. 23–28, 2011.

[13] F. Bonomi and C. Fellow, "The Smart and Connected Vehicle and the Internet of Things," Invited Talk, Workshop on Synchronization in Telecommunication Systems, 2013.

[14] Muhammad Edmerdash, Waleed khedr, Ehab Rushdy, An Overview of Cloud-Based Secure Services for Enterprise Drug–Drug Interaction Systems, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 2 , (2021) : 49-58 (Doi : https://doi.org/10.54216/IJWAC.020201)

[15] Noushini Nikeetha P. , Pavithra D. , Sivakarthiga K. , Karthika S. , Yashitha R. , Kirubasri G.V., A Survey on IoT based Wearable Sensor for Covid-19 Pandemic, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 2 , (2021) : 77-87 (Doi : https://doi.org/10.54216/IJWAC.020203)

[16] F. D. Da Cunha et al., "Data Communication in VANETs: A Survey, Challenges and Applications," INRIA Saclay; INRIA, Rocquencourt, France, 2014, Ph.D. Dissertation.

[17] H. Sodhro et al., "AI-Enabled Reliable Channel Modeling Architecture for Fog Computing Vehicular Networks," IEEE Wireless Communications, vol. 27, no. 2, pp. 14–21, 2020.

[18] F. Yang et al., "An Overview of Internet of Vehicles," China Communications, vol. 11, no. 10, pp. 1–15, 2014.

[19] S. Yu et al., "IOV-SMAP: Secure and Efficient Message Authentication Protocol for IOV in Smart City Environment," IEEE Access, vol. 8, pp. 167875–167886, 2020.

[20] Subhalaxmi Sahoo , Sudan Jha , Deepak Prashar, A novel approach for Spam Email Filtering Using Machine Learning, Journal of Cybersecurity and Information Management, Vol. 2 , No. 2 , (2020) : 44-57 (Doi : https://doi.org/10.54216/JCIM.020202)

[21] Ahmed N. Al Masri , Hamam Mokayed, An Efficient Machine Learning based Cervical Cancer Detection and Classification, Journal of Cybersecurity and Information Management, Vol. 2 , No. 2 , (2020) : 58-67 (Doi : https://doi.org/10.54216/JCIM.020203)

[22] S. Kuutti et al., "A Survey of the State-of-the-Art Localization Techniques and Their Potentials for Autonomous Vehicle Applications," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 829–846, 2018.

[23] V. Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021 ,PP. 42-52.

[24] R. Hussain and S. Zeadally, "Autonomous Cars: Research Results, Issues, and Future Challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1275–1313, 2019.

[25] Gajender Kumar, Vinod Patidar, Prolay Biswas, Mukta Patel, Chaur Singh Rajput, Anita Venugopal, Aditi Sharma, IOT enabled Intelligent featured imaging Bone Fractured Detection System, Journal of Intelligent Systems and Internet of Things, Vol. 9 , No. 2 , (2023) : 08-22 (Doi : https://doi.org/10.54216/JISIoT.090201)

[26] Alber S. Aziz, Moahmed Emad, Mahmoud Ismail, Heba Rashad, Ahmed M. Ali, Ahmed Abdelhafeez, Shimaa S. Mohamed, An Intelligent Multi-Criteria Decision-Making Model for selecting an optimal location for a data center: Case Study in Egypt, Journal of Intelligent Systems and Internet of Things, Vol. 9 , No. 2 , (2023) : 23-35 (Doi : https://doi.org/10.54216/JISIoT.090202)

[27] T. Jiang, H. Fang, and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640–4649, 2019.

DOI: https://doi.org/10.54216/JCIM.150126
Received: April 11, 2024 Revised: June 10, 2024 Accepted: August 08, 2024