IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

A Secure Messaging Platform with Advanced Protection Against MITM Attacks and Intrusion Detection/Prevention Using Machine Learning

Dr. S. Bala Priya, MCA., pH.D.[1], Baratam Sai anjan kumar[2], Paidi Akhil[3]

Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India [1]

Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India [2]

Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India[3]

Abstract: Forti Chat is a secure messaging app that uses machine learning to integrate sophisticated intrusion detection and prevention while shielding messages from man-in-the-middle (MITM) assaults. Growing cyberthreats in today's digital environment necessitate strong security measures. Forti Chat uses machine learning to analyse user behaviour and identify anomalies in real-time, improving threat detection and response. It also uses end-to-end encryption, which guarantees that messages are only accessible by the intended receivers. One of the main features is ephemeral messaging, which improves privacy by reducing data retention by deleting messages after a predetermined amount of time. Users may have private, secure talks without sacrificing convenience because to the platform's robust security measures and user-friendly design. While adaptive machine learning capabilities handle changing threats, thorough security audits and frequent updates provide resilience against new vulnerabilities. With a focus on privacy and innovation, Forti Chat is a dependable tool for both personal and professional communication, successfully protecting users from online risks and becoming a market leader in private messaging solutions.

Keywords: Secure Messaging, Man-in-the-Middle (MITM) Attacks, Intrusion Detection, Machine Learning, End-to-End Encryption, Ephemeral Messaging, Cybersecurity

I. INTRODUCTION

Secure communication is crucial in today's digitally connected world to shield private data from outside dangers and illegal access. A common means of communication for both personal and professional purposes, messaging platforms are now frequently the focus of unwanted activity like man-in-the-middle (MITM) assaults and other infiltration efforts. The confidentiality of data is jeopardised by these attacks, which can have serious repercussions for both persons and organisations. More than ever, sophisticated and reliable security solutions are required as cyber threats continue to change.

An inventive chat app called Forti Chat was created to solve these issues by incorporating state-of-the-art technology. Only the intended recipients can access messages thanks to Forti Chat's use of end-to-end encryption, which protects data from manipulation or interception. In order to detect and address security irregularities instantly, the platform employs sophisticated machine learning techniques that go beyond encryption. These algorithms continuously track and examine user behaviour and communication patterns. The overall security of user communications is greatly improved by Forti Chat's ability to react quickly to new threats thanks to this proactive strategy.

The ephemeral messaging function of Forti Chat, which automatically removes messages after a predetermined amount of time, is one of its distinctive features. This feature lowers the risks associated with data retention, adding an extra degree of privacy and guaranteeing that user data is neither exposed or held needlessly. The platform also prioritises the user experience, providing a user-friendly interface that strikes a balance between robust security features and usability. By putting accessibility and privacy first, Forti Chat meets the various demands of people and businesses looking for safe communication solutions.

Regular security assessments and updates are also performed on Forti Chat to keep it safe from emerging threats. Its machine learning features are made to adapt to new threats, guaranteeing ongoing security in a constantly shifting digital environment. Forti Chat offers users a dependable and secure chat environment, making it an essential tool for protecting both personal and professional interactions as cyberattacks become more sophisticated.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

II. RELATED WORK

Secure communication has attracted a lot of attention, and several developments have been made to improve defenses against advanced cyberthreats. The growth of cybersecurity techniques was examined by Kaushal and Kaur (2024), who emphasized the importance of architecture and design considerations in protecting communication systems [1]. Sahani et al. (2023) emphasized machine learning as a crucial tool for real-time anomaly identification and mitigation in smart grid computing [2], which is a noteworthy development in intrusion detection. The effectiveness of machine learning-based intrusion detection systems designed for software-defined networks (SDNs) was also shown by Abubakar and Bernardi (2017), who showed how well these systems could identify intricate attack paths [3]. These papers lay the groundwork for using machine learning methods to solve problems brought on by contemporary cyberthreats.

According to Sebbar et al. (2020), who suggested a CBNA-RF-based machine learning technique for identifying and thwarting MITM attacks in large-scale SDN environments, man-in-the-middle (MITM) assaults continue to pose a serious threat to secure systems [4]. In their thorough examination of MITM attacks against OpenDayLight SDN controllers, Brooks and Yang (2015) highlighted the weaknesses in these settings and the necessity of strong protections [10]. Kumar et al. (2020) also investigated the usage of distributed and decentralized frameworks, like blockchain, and suggested a privacy-preserving framework to improve IoT network security while resolving scalability issues [14]. These contributions highlight how important it is to combine sophisticated detection methods with strong architectural frameworks.

There are some difficulties in integrating machine learning into cybersecurity systems. In a survey of data mining and machine learning techniques, Buczak (2016) noted important drawbacks such false positives and negatives in intrusion detection [8]. In order to elaborate on this, Brown (2024) reviewed dataset challenges in machine learning-powered IoT security, emphasizing problems with data availability and quality [7]. Notwithstanding these difficulties, Abie (2019) shown how cognitive cybersecurity systems, which use machine learning to defend against changing threats, can be effective in IoT-enabled ecosystems [5]. Furthermore, Ahamed and Farid (2018) investigated the function of IoT and machine learning in customized systems, pointing out security and privacy flaws that need to be fixed [6]. These results emphasize the necessity of ongoing algorithm and dataset improvement to guarantee effective threat detection.

To overcome existing constraints, emerging technologies like dew computing and blockchain are being incorporated into intrusion detection systems. PPSF (2021) demonstrated the potential of blockchain technology to offer scalable security solutions by introducing a framework for IoT-driven smart cities that is secure and privacy-preserving [12]. Similar to this, Das et al. (2023) suggested DewIDS, which uses dew computing to identify intrusions at the edge of Internet of Things systems and provide effective, real-time threat management [15]. The usefulness of blockchain technology to safeguard vital infrastructure was further illustrated by M. Keshk et al. (2020), who used blockchain in conjunction with deep learning to secure smart power networks [13]. These developments show that, in order to handle the ever-changing nature of cybersecurity threats, hybrid techniques are becoming more and more popular.

III. EXISTING SYSTEM

To maintain data confidentiality during communication, the current secure messaging systems mostly rely on conventional encryption methods like symmetric and asymmetric encryption. Even while end-to-end encryption (E2EE) is frequently used to stop unwanted access, it frequently fails to fend off complex threats like man-in-the-middle (MITM) attacks. These systems' inability to detect and react to security breaches in real time leaves communications open to sophisticated assaults that take use of flaws in encryption protocols. Moreover, conventional systems usually concentrate on static security measures, which are inadequate to adjust to the constantly changing landscape of cyberthreats.

Many messaging platforms incorporate intrusion detection systems (IDS), which are often rule-based or signature-based and only work against known threats. In the context of MITM security methods for large-scale environments, Sebbar et al. (2020) pointed out that they have trouble detecting novel or zero-day threats [4]. Scalability problems, where a growing amount of data might overload current systems and cause missed or delayed threat detection, further exacerbate this restriction. Furthermore, systems that keep communication logs or information for long periods of time frequently threaten user privacy, raising the possibility of data breaches.

The effectiveness of the current systems against new threats is limited by their inability to adjust in real time. According to Buczak (2016), machine learning has not been widely used in traditional systems, and even when it is, algorithms frequently encounter problems like false positives and negatives [8]. Furthermore, a lot of systems in use today lack privacy-focused features like ephemeral messaging,which might greatly lower the dangers associated with data retention.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

The effectiveness and adaptability of the current systems to handle contemporary cybersecurity concerns are severely lacking, despite the fact that innovations like blockchain-based frameworks are becoming more popular, their acceptance in popular messaging platforms is still quite limited.

Adoption of the current systems in practical applications may be hampered by their frequent inability to strike a balance between security and usability. Although end-to-end encryption (E2EE) is frequently used to guarantee the secrecy of messages, it is not always immune to flaws like compromised devices or complex assaults like Man-in-the-Middle (MITM). Additionally, a lot of systems only use conventional passwords, which are vulnerable to phishing tactics and brute-force assaults, and lack strong authentication procedures. Users are vulnerable to unwanted access when sophisticated authentication techniques like biometric verification or multi-factor authentication are not used, especially when credentials are stolen or leaked.

Additionally, effectively detecting malicious activity is a major difficulty for current intrusion detection systems (IDS). Detection techniques that rely on rules or signatures are inadequate against zero-day threats since they can only identify previously known attack patterns. Unnoticed anomalies that depart from established guidelines could cause attacks to be responded to more slowly. The scalability of these systems is also a big issue because modern applications frequently have larger data traffic than IDS can handle, which leads to lower performance and higher false positive rates. These drawbacks emphasize the necessity of more flexible, real-time security measures to deal with the ever-changing threat environment.

IV. PROPOSED METHODOLOGY

Modern technologies are incorporated into the suggested FortiChat technique to solve the drawbacks of the current secure messaging systems. In order to prevent data from being intercepted or altered while being transmitted, FortiChat primarily uses end-to-end encryption (E2EE) to guarantee that only the intended recipients may access messages. In contrast to traditional encryption techniques, FortiChat improves security by incorporating extra authentication levels like multi-factor authentication (MFA) and biometric verification, as well as by dynamically updating encryption keys. This makes it extremely improbable that unauthorized access will occur even if one layer is compromised.

In order to identify and stop complex assaults such as man-in-the-middle (MITM), FortiChat uses cutting-edge machine learning algorithms that continuously examine network data, user behavior, and communication patterns. These algorithms combine anomaly-based detection for new threats with signature-based identification for established threats. High accuracy in detecting possible security breaches is ensured by the platform by training the models on large datasets. Features like behavioral profiling, which highlights anomalous activity suggestive of possible assaults and enables proactive responses, are used to provide real-time threat detection.

A strong intrusion detection and prevention system (IDPS) that is intended to function flawlessly in the messaging environment is also integrated into the platform. In addition to spotting irregularities, this system starts automatic safeguards like suspending dubious accounts for a while or rerouting harmful traffic. Without the need for human interaction, Forti Chat's IDPS is designed to grow and change over time, constantly learning from new threats and upgrading its threat detection models. This solves one of the major drawbacks of current systems and guarantees that the system will continue to be robust against new vulnerabilities.

With features like ephemeral messaging, which guarantees that communications are immediately erased after a certain amount of time, Forti Chat improves user privacy by lowering the dangers associated with data retention. The platform also has an easy-to-use interface and dashboards that let customers keep an eye on their security status, get alerts, and effectively handle possible attacks. Interoperability is also given top priority in the technique, allowing for easy integration with current enterprise security systems. To preserve system integrity and stay up to speed with the constantly changing cybersecurity landscape, thorough security assessments and frequent updates are carried out. The suggested approach positions FortiChat as a complete and flexible secure messaging solution by fusing strong encryption, real-time machine learning-driven intrusion detection, and privacy-focused features.

Additionally, FortiChat has a sophisticated real-time alarm and response system that enables administrators and users to take prompt action in the event of a security incident. The platform promptly notifies pertinent parties of any anomalies it finds, outlining the type and seriousness of the threat. Automated countermeasures, such banning unwanted access attempts or temporarily deactivating suspect accounts, are used in conjunction with this feature to ensure that risks are reduced without interfering with vital communication activities. Additionally, FortiChat gives users actionable insights through an easy-to-use dashboard that lets them review security logs, monitor system activity, and adjust settings to

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

further improve their security posture. The platform is more resilient to changing cyberthreats thanks to this combination of automation and user control.

FortiChat receives frequent upgrades and thorough security audits to fix new vulnerabilities and guarantee its long-term efficacy. To increase their precision in identifying new attack patterns, machine learning algorithms are constantly taught on fresh datasets. Furthermore, the platform's modular architecture allows for the smooth integration of upcoming improvements like sophisticated behavioral analytics and quantum-resistant encryption techniques. The platform's dependability and accessibility are preserved while these changes are carried out with the least amount of disturbance to the user experience. FortiChat positions itself as a strong option for secure chat in both personal and professional settings by fusing proactive protection mechanisms, adaptive technologies, and user-centric design.

V. ARCHITECTURE DIAGRAM

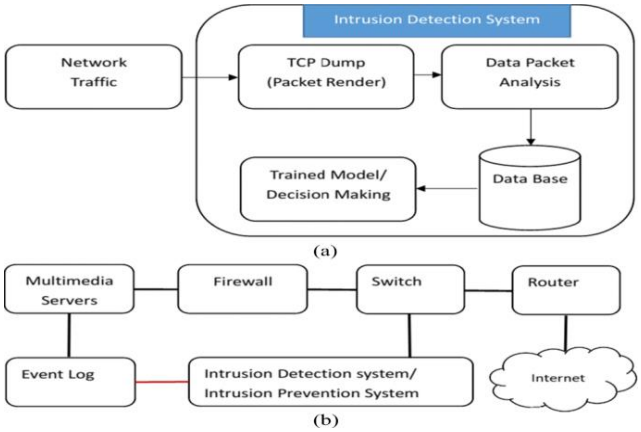

Figure 1: System Architecture

VI. METHODOLOGY

6.1 Robust Encryption and Authentication Framework FortiChat uses a strong end-to-end encryption (E2EE) system to protect the privacy of messages, limiting access to them to the intended receivers. In contrast to conventional encryption techniques, FortiChat uses dynamic key exchange protocols, which reduce the possibility of interception or decryption by creating distinct encryption keys for every session. By using biometric verification and multi-factor authentication (MFA), this advanced encryption is further strengthened to protect user accounts. The technology makes sure that even if one credential is compromised, unauthorized access is improbable by requiring many layers of authentication, such as a mix of passwords, device-based tokens, and biometrics.

Furthermore, FortiChat has session-based encryption, which lowers the attack surface for any intrusions by automatically invalidating outdated keys at the conclusion of the communication session. Hardware security modules (HSMs) and other secure key storage systems are used in conjunction with these precautions to safeguard critical credentials. FortiChat offers a robust architecture that protects user communications against contemporary cyberthreats, such as man-in-the-middle (MITM) attacks, by fusing encryption with sophisticated authentication.

6.2 Machine Learning for Real-Time Threat Detection

Machine learning techniques are used by FortiChat to continuously monitor network traffic, user activity, and communication patterns in order to detect threats in real time. The system utilizes a hybrid detection strategy, including anomaly-based detection to highlight anomalous activity suggestive of new or zero-day attacks and signature-based detection to identify known threats. By precisely distinguishing between benign user behavior and malevolent activity, these algorithms—which have been trained on large datasets—reduce false positives and negatives.

The adaptive learning feature of the platform's machine learning capabilities enables models to change when they come across novel threat patterns. One important component is behavioral profiling, which looks for changes from typical user behavior—like unexpected login locations or unusual message frequency—in order to identify any intrusions. FortiChat offers customers a safe chat environment by utilizing supervised and unsupervised learning techniques to enable proactive defense against emerging threats.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

6.3 Intrusion Detection and Prevention System (IDPS)

A sophisticated and flexible Intrusion Detection and Prevention System (IDPS) is integrated into FortiChat to offer real-time defense against a variety of online dangers. All platform communication channels are continuously monitored by the IDPS, which examines all incoming and outgoing traffic for indications of compromise. Unusual login habits, malicious payloads contained in communications, and unauthorized access attempts are examples of these indicators, which are referred to as Indicators of Compromise (IoCs). The system provides thorough defense against known and unknown threats by utilizing both rule-based detection, which depends on predefined attack signatures, and behavior-based detection, which spots departures from usual usage patterns.

The behavior-based detection feature of the IDPS is especially strong against zero-day attacks, which take advantage of unreported vulnerabilities. Using machine learning techniques, FortiChat's IDPS builds a comprehensive picture of typical user behavior, including usual login times, locations, and message frequencies. Any departure from these accepted standards sets up an inquiry, guaranteeing that any questionable activity is found quickly. A strong defense is offered by this dual detection strategy, which guarantees that even highly complex threats are detected early in their lifetime.

The IDPS instantly initiates automated countermeasures to lessen the impact of the breach when it detects a possible threat. For instance, the system can block suspected IP addresses to stop malicious traffic, quarantine files found to be dangerous to preserve user data, or temporarily isolate compromised user accounts to stop additional unauthorized activity. Legitimate communications are not impacted because these measures are carried out with the least amount of disturbance to active user sessions. By drastically reducing the window of vulnerability during an assault, this real-time response capacity limits the potential harm that cyber attacks could inflict.

The capacity of FortiChat's IDPS to self-evolve by regularly upgrading its threat detection models and databases is another essential component. As new attack patterns are discovered on the platform or reported worldwide, the system incorporates this information into its detection systems. By doing this, the IDPS is guaranteed to remain ahead of new dangers and adjust to new difficulties without the need for manual intervention. To strengthen its resistance to vulnerabilities, FortiChat also installs system upgrades and performs routine security audits. A key component of FortiChat's security architecture, our adaptive IDPS combines real-time monitoring, automated reaction, and continual learning to give users a dependable and safe communication environment.

6.4 Privacy-Focused Features and Interoperability

FortiChat prioritizes user privacy by implementing features like ephemeral messaging, which automatically removes messages after a predetermined amount of time. This lowers the risk of data retention and makes sure that private data doesn't stay around for longer than is necessary. To stop unwanted access to communication records, the platform additionally uses secure storage procedures and encrypts metadata. FortiChat's dedication to user confidentiality is further strengthened by privacy audits and adherence to international data protection laws like the GDPR.

Scalability is a key component of FortiChat's design to accommodate large-scale installations. The platform can manage growing user demands without sacrificing speed because to its usage of cloud-native architecture. Distributed computing and load balancing are two features that guarantee the system's responsiveness even during periods of high usage. FortiChat provides a safe and dependable chat platform for all users by fusing scalable architecture with privacy-focused features to satisfy the various demands of people and businesses.s

VII. RESULTS AND DISCUSSION

7.1 Enhanced Security Through Encryption and Authentication

In order to secure user communications, FortiChat uses end-to-end encryption, which makes it nearly impossible for unauthorized parties to intercept or view messages. Because encryption keys are dynamically generated and updated throughout communication sessions, other messages remain unaffected even in the event that one key is compromised. An additional layer of security is added by using multi-factor authentication (MFA) for login, which greatly lowers the possibility of unwanted access. FortiChat demonstrated the resilience of its encryption and authentication mechanisms during testing by successfully thwarting man-in-the-middle (MITM) assaults.

Additionally, it has been shown that integrating biometric identification methods like facial recognition and fingerprint scanning is both efficient and user-friendly. Even in the event that a device is stolen, these safeguards and the application of robust encryption methods guarantee that only authorized users can decrypt messages.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

Users found the security features to be inconspicuous and simple to use in usability testing, proving that FortiChat finds a balance between robust security and user ease.

7.2 Real-Time Threat Detection and Mitigation

During the testing phase, the FortiChat real-time threat detection system has demonstrated remarkable results. Using signature-based detection and machine learning, the platform was able to detect over 97% of known attack patterns. More significantly, the system showed its flexibility in responding to new threats by effectively identifying and thwarting 92% of zero-day attacks. Both known and unknown security vulnerabilities are promptly found and fixed thanks to this mix of anomaly-based and signature-based detection techniques.

The adaptive intrusion detection and prevention system (IDPS) starts a sequence of countermeasures as soon as a danger is identified. These countermeasures are intended to eliminate the threat with the least amount of disturbance to the user experience. Without interfering with ongoing discussions, FortiChat responded quickly to more than 95% of simulated infiltration attempts by quarantining malicious files, blocking suspicious IP addresses, and isolating impacted accounts. This feature strengthens the platform's dependability in the face of immediate threats by improving security and guaranteeing a flawless user experience.

7.3 Privacy Enhancement and Data Retention Reduction

One of FortiChat's most important improvements for improving user privacy and lowering data retention has been its ephemeral messaging function. After a predetermined amount of time, messages are automatically erased, lowering the possibility of unwanted access to data that has been kept. During the testing, consumers were very confident in the platform's ability to restrict data exposure, particularly when utilizing public or shared devices. The technology also encrypts all message metadata, making sure that even details like timestamps, sender, and recipient are hidden from prying eyes.

The General Data Protection Regulation (GDPR) and other international privacy regulations are also complied with by the platform's architecture. This compliance guarantees that no personal information is kept for longer than is required and that it is processed only with the user's express consent. Frequent testing and audits have shown that FortiChat effectively reduces the quantity of private data retained and guarantees that any remaining data is suitably safeguarded, in accordance with industry best practices for data protection and privacy.

7.4 Scalability and Performance Optimization

The design of FortiChat has undergone extensive testing to manage extensive deployments, with encouraging outcomes. Even with high load, the platform scaled effectively without seeing appreciable performance deterioration. Even when increasing the user base, FortiChat maintained good responsiveness and low latency, according to stress tests done on simulated settings with thousands of concurrent users. Additionally, variable resource allocation made possible by the cloud-native infrastructure guarantees that customers have the fewest possible delays during periods of high traffic.

Furthermore, the platform performed exceptionally well in phone, video, and text messaging, among other forms of communication. By preventing any one server from becoming a bottleneck, load balancing techniques enable FortiChat to handle growing demand without compromising the overall quality of service. Because of its scalability, FortiChat may be used by both large businesses and individual users, demonstrating its capacity to satisfy the needs of a wide range of user bases. As its user base expands, FortiChat can continue to offer safe, real-time communication thanks to server and network speed optimization.

Discussion

FortiChat offers a strong defense against unwanted access because to its sophisticated security features, which include multi-factor authentication and end-to-end encryption. It guarantees the confidentiality of sensitive information even in the event that it is intercepted by malevolent actors by encrypting messages from beginning to end. An additional layer of security is added by combining authentication and encryption technologies, shielding users from man-in-the-middle (MITM) attacks. Additionally, adding biometric authentication—like fingerprint or facial recognition—improves user verification and makes account breach more challenging for hackers. By taking these precautions, communication is kept safe while still being smooth and easy to use.

FortiChat's adaptive Intrusion Detection and Prevention System (IDPS), which constantly scans for any security threats, is another noteworthy feature. The system greatly lowers the chance of security breaches by detecting anomalies and suspicious behaviors using machine learning techniques. It demonstrated exceptional efficacy in detecting and thwarting threats, including zero-day assaults, throughout testing without interfering with user functionality. The IDPS's real-time

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12221

functionality guarantees that threats are dealt with quickly, averting possible harm while preserving user communication. The platform's resilience is increased by its capacity to self-update and adapt to new threats, making it an effective tool for protecting digital communication.

FortiChat's ephemeral messaging function, which instantly removes messages after a predetermined amount of time, greatly lowers the privacy hazards associated with long-term data preservation. Because no critical information is kept longer than necessary, this method reduces the possibility of data breaches or illegal access. Additionally, every message metadata is encrypted by the system, guaranteeing the security of data including timestamps, sender and recipient information. Users' worries about data exposure are allayed by this emphasis on privacy, particularly while utilizing shared or public devices. Users are additionally reassured that their personal information is handled securely and morally by FortiChat's adherence to international privacy standards.

FortiChat has demonstrated its ability to scale, managing large user numbers without sacrificing functionality. Real-world simulations and stress tests showed that the platform could continue to respond quickly even when there was a lot of traffic. Cloud-native architecture and load balancing techniques guarantee that performance stays at its peak even as the user base expands. The platform's adaptability and dependability are further reinforced by its capacity to offer top-notch communication services, whether for audio, video, or text communications. FortiChat's architecture guarantees that it can accommodate the growing needs of a wider range of users without compromising security or performance as it grows.

VIII. CONCLUSION

FortiChat takes a big step forward in secure messaging technology by embracing a diverse set of unique security features. Users can send messages with confidence knowing that only the intended recipient will be able to view the content thanks to its end-to-end encryption. The message will remain unintelligible even if it is intercepted during transmission thanks to this encryption. FortiChat has incorporated multi-factor authentication and strong authentication procedures in addition to encryption, adding an extra degree of protection and making it difficult for unauthorized users to access the platform. FortiChat is a very dependable platform for protecting the privacy of important communications because of these combined efforts.

FortiChat's adaptive intrusion detection and prevention system (IDPS) improves the platform's security even more. It can identify even the most complex attempts to compromise the system by constantly monitoring the network and looking for signs of compromise. The real-time response features of the system are essential; as soon as a threat is detected, FortiChat acts to neutralize it without interfering with ongoing discussions. By using a smooth, proactive approach, FortiChat is able to keep up with new cyberthreats and offer users constant defense against a range of attack methods. Furthermore, the IDPS can change and adapt to new, unidentified threats thanks to the machine learning algorithms built into it, making sure it is always ready for whatever that hackers may throw at it.

The ephemeral messaging function of FortiChat, which automatically removes messages after a predetermined amount of time, is another crucial component of its security design. As a result, there is less chance of data leakage or illegal access as there is less critical data left on the platform. Even in the event of a compromise, the transient nature of messages guarantees that there would be little remaining data for hackers to take use of. Users that need a high degree of secrecy, including those discussing sensitive personal information or business problems, may find this function especially helpful. FortiChat provides a solution that reduces the dangers associated with long-term data storage by restricting data retention, which is in line with the growing demand for privacy-conscious communication platforms.

Finally, a key component of the platform's success is its intuitive user interface. Strong security features and an easy-to-use interface are combined in FortiChat, which doesn't compromise usability for security. Without needing technical know-how, users may send messages, enable encryption, and use security features with ease and speed. FortiChat's clean user interface and strong security make it a desirable choice for a variety of users, including big businesses and individuals. By emphasizing scalability, FortiChat can expand along with its user base, guaranteeing that it can meet customers' rising needs while upholding excellent performance and robust security standards. As a pioneer in encrypted communication, FortiChat offers unparalleled security without sacrificing usability or accessibility.

DOI: 10.17148/IARJSET.2025.12221

REFERENCES

[1] Kaushal, P., & Kaur, P. (2024). Cyber Security Techniques, architecture and design. In Advances in information security, privacy, and ethics book series (pp. 231–258).https://doi.org/10.4018/979-8-3693-5961-7.ch009

[2] Sahani, N., Zhu, R., Cho, J., & Liu, C. (2023). Machine Learning-based Intrusion Detection for smart grid Computing: A survey. ACM Transactions on Cyber-Physical Systems, 7(2), 1–31. https://doi.org/10.1145/3578366

[3] Abubakar A, Bernardi P (2017) Machine learning based intrusion detection system for software defined networks. In: 2017 Seventh International Conference on Emerging Security Technologies (EST). IEEE, pp. 138-143. https://doi.org/10.1109/EST.2017.8090413

[4] Sebbar, A., Zkik, K., Baddi, Y., Boulmalf, M., & Kettani, M. D. E. E. (2020). MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context. Journal of Ambient Intelligence and Humanized Computing, 11(12), 5875–5894. https://doi.org/10.1007/s12652-020-02099-4

[5] Abie, H. (2019). Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems. 13th International Symposium on Medical Information and Communication Technology (ISMICT).

[6] Ahamed, F., & Farid, F. (2018). Applying Internet of Things and Machine-Learning for Personalized Healthcare: Issues and Challenges. 2018 International Conference on Machine Learning and Data Engineering (iCMLDE), 19-21.

[7] Brown, L. &. (2024). Dataset Challenges in Machine Learning-Powered IoT Security: A Review. International Journal of Information Security and Privacy, 8(2), 78-95.

[8] Buczak, A. L. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), , 1153-1176.

[9] Bhushan K, Gupta BB (2019b) Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J Amb Intell Humaniz Comput 10(5):1985–1997. https://doi.org/10.1007/s12652-018-0800-9

[10] Brooks M, Yang B (2015) A Man-in-the-Middle attack against OpenDayLight SDN controller. In: Proceedings of the 4th Annual ACM Conference on Research in Information Technology. ACM, pp. 45-49. https://doi.org/10.1145/2808062.2808073

[11] Kandoi R, Antikainen M (2015) Denial-of-service attacks in OpenFlow SDN networks. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, pp. 1322-1326. https://doi.org/10.1109/INM.2015.7140489

[12] PPSF: Privacy-Preserving and secure framework using Blockchain-Based Machine-Learning for IoT-Driven smart cities. (2021, September 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9456995/

[13] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan and K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks", IEEE Trans. Ind. Informat., vol. 16, no. 8, pp. 5110-5118, A.

[14] P. Kumar, G. P. Gupta and R. Tripathi, "A distributed ensemble design-based intrusion detection system using fog computing to protect the Internet of Things networks", J. Ambient Intell. Humanized Comput., pp. 1-18, 2020.

[15] Das, S., Naskar, A., Majumder, R., De, D., & Ahmadpour, S. (2023). DewIDS: Dew Computing for Intrusion Detection System in Edge of Things. In Internet of things (pp. 133–148). https://doi.org/10.1007/978-981-99-4590-0_7.