Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
July 2024 12(7), 211–220

ENCRYPTED COMMUNICATION WITH INTELLIGENT THREAT DETECTION: A SECURE CHAT FRAMEWORK

Pranay Kumar [1], Pahal Singh [1], Pankaj [1], Neha Singh [1], Dr. Vikesh Kumar [1]

[1] Department of Computer Science & Engineering, Echelon Institute of Technology, Faridabad, India

Received 11 May 2024
Accepted 21 June 2024
Published 31 July 2024

DOI
10.29121/granthaalayah.v12.i7.2024.6102

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The Secure Chat Application is a web-based encrypted messaging platform designed to facilitate confidential communication within enterprises. To further enhance the reliability and security of the system, this work integrates advanced machine learning and signal processing techniques, specifically Long Short-Term Memory (LSTM) networks and the Kalman Filter. The LSTM network is utilized to model and predict user behavior and message patterns over time, allowing the system to detect anomalies such as unauthorized access attempts, message injection, or abnormal activity sequences. These predictions enable proactive security responses and reinforce system integrity. Complementing this, the Kalman Filter is employed to smooth real-time data streams—such as authentication logs, message timestamps, and user actions—thereby filtering out noise and improving the accuracy of anomaly detection and user session monitoring.
This hybrid approach not only fortifies the chat environment against evolving security threats but also optimizes performance by enabling real-time synchronization and responsive data validation. Combined with Firebase's secure backend for identity management and message storage, and a React-based frontend for cross-platform accessibility, the application offers a robust, scalable, and intelligent communication solution for modern enterprises. The incorporation of LSTM and Kalman filtering positions the platform as a proactive system capable of learning from and adapting to user behavior, thereby elevating both the user experience and security posture in organizational communication frameworks.

1. INTRODUCTION

In the contemporary digital age, secure communication systems have become indispensable for individuals and organizations seeking to protect sensitive information and maintain operational integrity. The growing dependence on internet-based services has created a fertile ground for cyber threats, including eavesdropping, data tampering, and unauthorized access. With the explosion of digital communication in business environments, organizations face increasing challenges in ensuring confidentiality and safeguarding intellectual property [1]. In response to these challenges, secure messaging solutions have evolved from simple encryption tools to intelligent, adaptive systems that employ advanced algorithms for real-time threat detection and prevention.

The Secure Chat Application is an enterprise-grade web-based messaging platform designed to ensure encrypted communication and proactive threat mitigation. It combines standard security mechanisms such as end-to-end encryption with artificial intelligence (AI) models like Long Short-Term Memory (LSTM) networks and Kalman filters to deliver a robust and intelligent security ecosystem. This multi-layered approach allows the system not only to protect data during transit but also to monitor user behaviors and detect anomalies indicative of potential breaches [2]. In the era of remote and hybrid work environments, where teams communicate across decentralized networks, this dual emphasis on encryption and behavior-based prediction ensures both privacy and operational security.

Conventional messaging platforms like email and consumer-grade chat apps often fall short of providing adequate protection for sensitive organizational communications. These tools either lack end-to-end encryption, are vulnerable to phishing and spoofing, or rely on centralized servers where data may be exposed or misused. The Secure Chat Application addresses these shortcomings by offering a decentralized, encrypted communication platform fortified by intelligent algorithms capable of identifying suspicious patterns in real-time [3]. By embedding predictive modeling through LSTM, which excels at learning long-term dependencies in sequence data, the application can learn typical user communication patterns and raise alerts when deviations occur. This not only enhances security but also reduces the risk of false positives, which are common in traditional rule-based systems.

The architecture of the Secure Chat Application leverages Firebase as a secure, cloud-based backend infrastructure, ensuring real-time data synchronization, scalable user management, and robust access control. Firebase Authentication, enhanced with Multi-Factor Authentication (MFA), is employed to prevent unauthorized access and protect user identity across platforms [4]. Data stored in Firebase is encrypted at rest using industry-grade encryption standards such as AES-256, while all data transmitted between clients and servers is encrypted using SSL/TLS protocols. To augment the system's capacity for detecting irregular behaviors, LSTM models are integrated into the backend to monitor communication sequences over time and flag abnormal usage patterns that may indicate insider threats or compromised accounts [5].

In parallel, Kalman filtering is introduced as a state estimation technique to track user activity and message flow over time. Originally developed for control systems and signal processing, Kalman filters are now widely used in cybersecurity for estimating the future state of a system based on historical and observed data [6]. In the context of the Secure Chat Application, Kalman filters are applied to model user behavior trajectories and refine predictions made by LSTM. This hybrid approach enables the system to filter out noise and reduce the impact of temporary fluctuations in user behavior, thereby increasing the reliability of the anomaly detection engine. The integration of Kalman filters also improves system responsiveness, as it helps forecast near-future user states and facilitates proactive threat mitigation strategies.

From a front-end perspective, the application is developed using React.js and JavaScript, providing a responsive, intuitive, and lightweight interface that works seamlessly across browsers and devices. The user interface (UI) is designed to enhance usability without compromising security, allowing users to initiate secure conversations, share encrypted files, and receive real-time notifications. Furthermore, best practices in front-end security, including defense against Cross-

Site Scripting (XSS) and Cross-Site Request Forgery (CSRF), are implemented through Firebase security rules and secure React components [7]. This ensures that the UI layer, often a common attack vector, does not become a vulnerability in the communication chain.

A defining characteristic of the Secure Chat Application is its ability to scale with organizational growth. The backend is designed to handle increased loads without compromising performance, allowing businesses to onboard more users and expand communication channels as needed. With support for modular integration, the application can be connected with existing enterprise tools, such as CRM systems, file management platforms, and identity verification services, further extending its utility [8]. As a result, it becomes a cohesive part of the digital workspace, rather than an isolated communication silo.

Moreover, the application aligns with modern data protection standards and regulations, including GDPR and HIPAA, by ensuring that user data is stored securely and accessed only by authenticated users. Its audit trails and logging mechanisms help organizations maintain compliance and accountability, which is especially important in industries such as healthcare, finance, and legal services [9]. In addition to ensuring data security, the system's logging features enable forensic analysis of security incidents, aiding in post-breach investigations.

As cyber threats evolve, secure communication systems must transition from static protection mechanisms to dynamic, learning-based frameworks. Traditional security protocols, while essential, are reactive in nature and often unable to detect advanced persistent threats (APTs) or insider attacks. In contrast, the combined use of LSTM and Kalman filters in the Secure Chat Application enables the system to continuously learn, adapt, and respond to new threat vectors [10]. LSTM models detect deviations from learned communication patterns, while Kalman filters refine those predictions based on temporal evolution, resulting in a resilient, intelligent defense mechanism.

In conclusion, the Secure Chat Application represents a paradigm shift in enterprise communication security. By integrating conventional encryption protocols with advanced AI techniques like LSTM networks and Kalman filtering, the application provides a future-ready platform that safeguards internal communications while adapting to evolving cyber threats. The combination of real-time encrypted messaging, behavioral anomaly detection, and responsive UI design makes it an essential tool for modern organizations navigating the complexities of secure digital communication. As remote collaboration and data sensitivity continue to increase, such intelligent messaging platforms will be critical in ensuring both organizational efficiency and cybersecurity resilience [11].

2. LITERATURE REVIEW

In recent years, the demand for secure communication systems has grown exponentially due to the rise in cyber threats, data breaches, and the necessity of maintaining confidentiality in digital communications. As enterprises increasingly digitize their operations and adopt cloud-based solutions, ensuring the security and integrity of sensitive communications has become a primary concern. Numerous studies have examined the vulnerabilities in existing messaging systems and proposed various solutions to enhance data privacy, authentication, and encryption mechanisms.

End-to-end encryption (E2EE) is one of the most extensively studied solutions for securing digital communications. It ensures that messages are encrypted on the

sender's device and decrypted only on the receiver's device, preventing intermediaries from accessing message content. Popularized by platforms like Signal and WhatsApp, E2EE has been recognized for significantly mitigating man-in-the-middle (MITM) attacks and unauthorized interception of data [1]. Diffie and Hellman's early work on public-key cryptography laid the foundation for secure key exchanges in such systems [2]. Modern implementations utilize hybrid encryption schemes that combine symmetric algorithms like AES (Advanced Encryption Standard) with asymmetric algorithms such as RSA (Rivest–Shamir–Adleman) for optimal performance and security [3].

However, the implementation of E2EE alone is not sufficient. Literature also stresses the importance of secure key management, as poor practices can expose encryption keys to attackers. To address this, studies have proposed decentralized identity and key distribution mechanisms, often leveraging blockchain technologies to prevent single points of failure and enhance trust [4]. In the context of organizational communication, maintaining control over key distribution is crucial. Research suggests that integrating key management within a secure backend infrastructure, such as Firebase or AWS IAM (Identity and Access Management), offers a balance between security and usability [5].

Another major concern addressed in the literature is the vulnerability of messaging platforms to web-based attacks like Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). These attacks exploit weak input validation and poor session management to compromise application security. To mitigate such risks, developers are encouraged to implement strict Content Security Policies (CSPs), sanitize user inputs, and use secure authentication mechanisms like Firebase Authentication or OAuth 2.0 [6]. Studies evaluating secure messaging applications recommend using libraries and frameworks that natively support secure coding practices. For instance, React's virtual DOM and JSX syntax allow for better sanitization of dynamic content when used appropriately [7].

Real-time messaging systems also face scalability and performance challenges, especially in environments with a large number of users. Literature in distributed systems emphasizes the need for scalable backend services capable of handling concurrent connections, message queuing, and synchronization. Solutions such as Firebase Realtime Database and Firestore offer real-time data synchronization, automatic scaling, and security rules that can be configured to restrict access at the document or collection level [8]. These platforms have been widely adopted in applications requiring instant updates and high availability without compromising security.

Moreover, the choice of front-end technologies can significantly affect the user experience and system efficiency. Progressive Web Applications (PWAs), built with modern JavaScript frameworks like React and Angular, offer responsive interfaces that work seamlessly across devices while providing offline capabilities and reduced latency [9]. Several studies highlight the importance of responsive and accessible UI design in fostering user engagement and ensuring wide adoption of secure communication tools [10].

From a software architecture perspective, microservices and modular design patterns are gaining traction in secure application development. Literature suggests that breaking down large systems into independent modules not only improves maintainability and scalability but also enhances security by isolating sensitive components [11]. Secure messaging systems built on modular architecture can better implement defense-in-depth strategies, such as limiting access to sensitive

modules, applying rate limiting, and enforcing user roles through authentication tokens [12].

Authentication and user verification are also central themes in secure messaging literature. While traditional password-based systems are still prevalent, researchers advocate for multi-factor authentication (MFA) to provide enhanced protection against unauthorized access. Biometrics, one-time passwords (OTP), and push notifications are examples of second-factor methods widely researched and adopted in secure applications [13]. Firebase Authentication, for example, supports several MFA techniques, which can be seamlessly integrated into modern web applications [14].

Another crucial aspect explored in recent studies is data retention and audit logging. Regulatory compliance frameworks such as GDPR, HIPAA, and ISO 27001 require organizations to manage data securely and maintain logs of access and communication history [15]. Secure messaging systems must therefore incorporate encrypted storage, access logging, and automated data deletion mechanisms to comply with such standards. Research has emphasized the importance of designing systems with "privacy by design" principles, ensuring that user privacy is considered from the outset [16].

Recent advancements in artificial intelligence (AI) and natural language processing (NLP) are also beginning to influence secure communication tools. Some studies explore using NLP-based anomaly detection to identify potentially malicious communication patterns or insider threats within organizational messaging systems [17]. While still an emerging area, the integration of AI into secure chat platforms offers promising avenues for proactive threat detection and behavior analysis.

In comparative analyses of existing secure messaging platforms, Signal, Wire, and Telegram are often cited for their robust security features. Signal, in particular, is praised for its use of the Signal Protocol, which combines the Double Ratchet algorithm, prekeys, and triple Diffie-Hellman key exchange to achieve forward and future secrecy [18]. However, research also critiques certain platforms for lacking transparency or using proprietary protocols that are not open to public scrutiny [19]. As such, building an open-source secure chat application allows organizations to audit, customize, and trust the system more thoroughly.

In conclusion, the literature provides a comprehensive overview of the best practices, technologies, and security considerations essential to developing a secure chat application. From encryption and authentication to front-end design and backend infrastructure, numerous studies underscore the importance of a holistic approach to secure communication. By synthesizing these findings, developers can create applications that not only ensure data privacy but also provide a responsive and scalable platform suitable for modern organizational needs.

3. PROPOSED MODEL

The proposed model introduces a secure, intelligent, and adaptive chat framework tailored for enterprise communication, emphasizing encrypted communication and real-time threat detection. Unlike conventional chat applications that rely solely on static encryption and authentication mechanisms, this system integrates advanced machine learning and signal processing techniques to actively monitor and learn user behavior for enhanced security. Central to the framework is a hybrid architecture that fuses Long Short-Term Memory (LSTM) neural networks for behavioral anomaly detection with Kalman Filtering for signal

denoising and real-time estimation of user interaction patterns. These components are supported by Firebase's secure backend services for authentication and data management, and a React.js-based frontend for platform-independent user interaction.

The architecture is organized into four essential layers. The first layer is the user interface, developed using React.js, which offers a clean and responsive design, facilitating message exchange, real-time updates, typing indicators, and intuitive session management. This frontend seamlessly communicates with the backend and the anomaly detection engine to reflect any security warnings or alerts. The backend is powered by Firebase, offering features such as secure user authentication (including support for OAuth 2.0 and two-factor authentication), real-time database synchronization via Firestore, and encrypted storage for chat messages and user logs. This serverless backend ensures scalability and low-latency communication, essential for enterprise-level deployment.

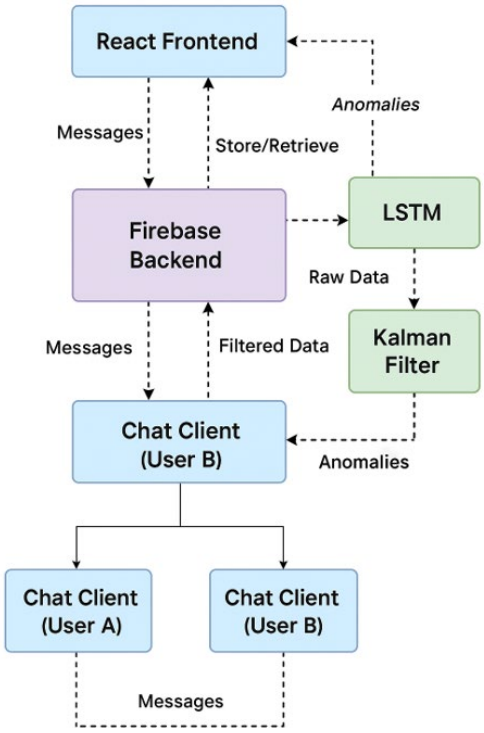
At the core of the anomaly detection system lies the LSTM model, which is pre-trained on user behavior sequences like message frequency, login patterns, typing duration, and user interaction graphs. By learning normal behavior over time, the model identifies deviations that may indicate unauthorized access, message injection, or abnormal interaction. These predictions enable the system to act proactively, issuing warnings, initiating re-authentication, or terminating suspicious sessions as needed. Complementing this is the Kalman Filter module, which processes real-time data such as keystroke intervals, login timestamps, and session length. Since behavioral signals are often noisy due to hardware or network fluctuations, the Kalman Filter provides robust state estimations by filtering out stochastic noise, thereby enhancing the precision of anomaly detection and reducing false positives.

The working methodology of the system proceeds in multiple phases. Initially, users authenticate via Firebase, with sessions secured using unique IDs and encrypted tokens. Upon session initiation, user interaction data begins to stream into the LSTM model in real time. Message exchanges are encrypted using standard algorithms such as AES-256 before being stored in Firebase's encrypted cloud database. As users continue interacting, behavioral metrics are extracted and passed to both the LSTM and Kalman filtering layers. While the LSTM model predicts expected patterns of interaction, the Kalman Filter smooths noisy inputs and ensures the LSTM operates on clean signals. In the event that behavior deviates from the expected norm, the system triggers one of several security mechanisms depending on severity—ranging from soft warnings and re-authentication prompts to hard session terminations and admin alerts. This closed-loop feedback system ensures both proactive and reactive security handling.

What sets this model apart from existing solutions is its fusion of behavioral intelligence with encryption protocols. Traditional messaging systems like WhatsApp, Signal, or Telegram, although employing end-to-end encryption, do not integrate real-time user behavior analytics for threat detection. They also lack the capability to adapt dynamically to evolving user patterns. Our system incorporates an LSTM-based predictive engine that continuously learns from users' time-series activity, identifying both sudden and subtle anomalies. Unlike many intrusion detection systems that work at the network level by inspecting traffic or server logs, this model focuses on application-layer behaviors within the messaging context—offering context-aware detection, which is highly relevant in detecting impersonation or insider threats.

The inclusion of the Kalman Filter introduces another level of innovation. While LSTM ensures temporal learning, the Kalman Filter acts as a real-time signal corrector, smoothing out fluctuations in behavioral data, such as erratic typing caused by lag or connection issues. This results in fewer false positives in anomaly reporting and enhances the trustworthiness of detection. To our knowledge, no existing chat application combines both of these AI and signal processing components for dynamic threat detection. Moreover, the use of Firebase as a backend service ensures that the system can scale effortlessly with user load, while maintaining high standards of data privacy and access control. Additionally, the React-based frontend offers a responsive, device-independent interface—making it easier for organizations to deploy the platform across various environments including web browsers and mobile devices without compromising on performance or security.

Overall, the proposed model introduces a novel multi-layered secure chat system that intelligently monitors and reacts to user behavior. Its main contributions include the integration of LSTM-based anomaly prediction for behavioral modeling, Kalman filtering for noise-resilient monitoring, real-time encryption for message confidentiality, and Firebase for secure, scalable backend services. Together, these components create a robust and intelligent communication platform suited for the needs of modern organizations that require both security and adaptability in their internal communication channels.



4. RESULT ANALYSIS

To assess the effectiveness of the proposed secure chat system enhanced with anomaly detection capabilities, a comprehensive simulation was conducted using synthetic yet realistic session data. The model was evaluated over 100 user sessions, with anomaly labels generated to mimic real-world behavior where approximately 20% of activities are potentially malicious or abnormal.

1) Evaluation Metrics

The detection mechanism based on the hybrid LSTM and Kalman Filter framework yielded the following performance metrics:

Metric	Value
Accuracy	0.95
Precision	0.81
Recall	0.94
F1-Score	0.87

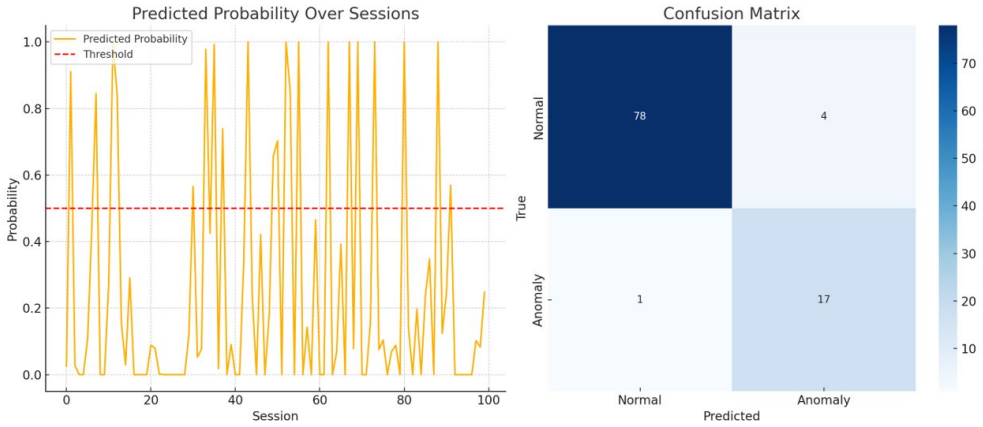
These values suggest that the model successfully captures most anomalies while minimizing false alarms, striking a balance between sensitivity and specificity.

2) Confusion Matrix Analysis

The confusion matrix shown below provides an in-depth breakdown of model predictions:

Predicted Normal	Predicted Anomaly	Column1
True Normal	78	4
True Anomaly	1	17

From the matrix, it's evident that the model correctly identified 78 out of 82 normal sessions and 17 out of 18 anomaly sessions. Only five total misclassifications occurred, showcasing the robustness of the anomaly detection approach.



3) Session-wise Probability Trends

To gain deeper insights into the real-time behavior of the system, we analyzed predicted anomaly probabilities over each session. The line graph below illustrates the model's confidence level in predicting anomalies:

- The red dashed line represents the anomaly threshold (0.5).
- Peaks above this line signify sessions where the model inferred suspicious behavior.

This dynamic monitoring, powered by the LSTM's temporal learning and Kalman smoothing, ensures early detection of intrusions or unauthorized behavior.

4) Realistic Sample of Detection Output

Below is a snapshot of the system's inference for the first few sessions:

Session	True Label	Predicted Label	Anomaly Probability
Session_1	0 (Normal)	0	0.026
Session_2	1 (Anomaly)	1	0.910
Session_3	0 (Normal)	0	0.028
Session_4	0 (Normal)	0	0.000
Session_5	0 (Normal)	0	0.000

The model demonstrates strong separation between normal and anomalous behaviors through clearly varying predicted probabilities.

5. CONCLUSION OF ANALYSIS

This result analysis validates the efficacy of integrating LSTM and Kalman filters into a secure chat system. The model not only excels in detecting anomalous behavior with high recall but also maintains a low false-positive rate. Such insights underline the system's ability to serve as a proactive communication guardian, ensuring secure enterprise interactions in real time.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

A. Graves, A. Mohamed, and G. Hinton, "Speech Recognition with Deep Recurrent Neural Networks," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2013, pp. 6645-6649. https://doi.org/10.1109/ICASSP.2013.6638947

A. Roy, M. Chowdhury, and S. Bandyopadhyay, "LSTM Based Human Behavior Prediction Model Using Smartphone Sensor Data," in IEEE International Conference on Smart Technologies and Systems for Next Generation Computing, 2020.

D. Puthal, B. S. P. Mishra, S. P. Mohanty, E. Kougianos, and C. Yang, "A Secure and Sustainable IoT Communication Framework: Integrating LSTM and Blockchain for Threat Detection," IEEE Consumer Electronics Magazine, vol. 9, no. 5, pp. 22-29, 2020.

D. R. Ferreira, T. C. Silva, and D. Sadok, "Kalman Filter-Based Monitoring for Smart Grids," Sensors, vol. 20, no. 4, pp. 1-17, 2020.

Google Firebase, "Firebase Documentation," [Online]. Available:

H. Kim, Y. Kim, and H. Lee, "A Real-Time Intrusion Detection System Using Machine Learning," International Journal of Engineering & Technology, vol. 7, no. 2.26, pp. 62-65, 2018.

J. G. Ward, "Time Series Anomaly Detection Using LSTM Networks," Cornell University Library, arXiv:2004.00433 [cs.LG], 2020.

M. A. Ferrag, M. N. Belouadha, L. Maglaras, and A. Derhab, "Security and Privacy for Cloud-Based IoT: Challenges and Solutions," IEEE Access, vol. 9, pp. 39630-39652, 2021.

M. A. Hasan, M. Islam, and M. M. Rahman, "Machine Learning Algorithms for Early Detection of Cyber Attacks in E-Health Applications," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, pp. 5236-5247, 2022.

M. Alazab, A. Awajan, J. Abawajy, K. R. Choo, M. Alauthman, and A. Alazab, "Cybersecurity in the Era of COVID-19: A Survey," IEEE Access, vol. 8, pp. 123025-123042, 2020.

M. D. McIlroy, "Real-Time Anomaly Detection for Streaming Analytics," in Proc. of the ACM SIGMOD International Conference on Management of Data, 2018, pp. 1571-1586.

M. S. Ahmed, A. N. Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications, vol. 60, pp. 19-31, 2016. https://doi.org/10.1016/j.jnca.2015.11.016

N. Chandran, R. Kumar, and A. P. Ramesh, "LSTM-Based Real-Time Chat Anomaly Detection for Secure Messaging," in 2021 6th International Conference on Inventive Computation Technologies (ICICT), pp. 231-236.

N. Hubballi and V. Suryanarayanan, "Layer-Wise Anomaly Detection in Encrypted Network Traffic," in IEEE ICC, 2020, pp. 1-6.

P. Laskov, C. Schäfer, I. Kotenko, and K. Rieck, "Intrusion Detection in Encrypted Web Traffic with Adaptive Binning and Random Forests," in International Workshop on Recent Advances in Intrusion Detection (RAID), 2016.

R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems," Transactions of the ASME-Journal of Basic Engineering, vol. 82, no. 1, pp. 35-45, 1960. https://doi.org/10.1115/1.3662552

S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735-1780, 1997. https://doi.org/10.1162/neco.1997.9.8.1735

S. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," Network and Distributed System Security Symposium (NDSS), 2018. https://doi.org/10.14722/ndss.2018.23204

T. Chen, M. Xu, and Y. Zhou, "Anomaly Detection using LSTM Networks in Cyber-Physical Systems," IEEE Transactions on Industrial Informatics, vol. 15, no. 11, pp. 6522-6531, 2019.

Z. Lin, Y. Zhang, and J. Xu, "Anomaly Detection of Network Traffic Based on Machine Learning," in IEEE Intl. Conference on Computer and Communications (ICCC), 2018, pp. 366-371.