LockTalk: A Basic Secure Chat Application

1st Aashi Sharma
Department of Cyber Security
Noida Institute of Engineering & Technology
Greater Noida, India
aashisharma2134@gmail.com

2nd Sumit Sharma
Department of Cyber Security
Noida Institute of Engineering & Technology
Greater Noida, India
sssumitsssharma@gmail.com

3rd Puneet Garg
Department of CSE - AI
KIET Group of Institutions
Delhi NCR, Ghaziabad
puneetgarg.er@gmail.com

4th Parul Bhardwaj
Department of Applied Science
SAITM, Gurugram
Delhi NCR, India
parul.bhardwaaj@gmail.com

Abstract **- In today's world, ensuring the privacy and security of online messages is increasingly important, given our reliance on digital communication. Many widely used messaging applications, however, lack robust protective measures. This deficiency exposes users to risks such as data breaches, unauthorized surveillance, and intrusions by malicious actors. LockTalk is a chat application designed to address these concerns by prioritizing security. It offers a straightforward tool that employs encryption to safeguard conversations. This article will explore what distinguishes LockTalk, including its approach to secure data handling, its use of end-to-end encryption, and its method for verifying user identity. It will also examine how LockTalk could contribute to secure communication practices.**

LockTalk places a strong emphasis on user privacy. It utilizes encryption to maintain the confidentiality of messages. In contrast to many applications that retain chat histories on large central servers, LockTalk adopts a minimal-storage approach to reduce the likelihood of security vulnerabilities. This discussion will cover the challenges associated with securing messages, provide a comparison between LockTalk and other encrypted messaging platforms, and identify areas where it might enhance its offerings. LockTalk seeks to serve as a practical option for both personal and professional communication, improving security without compromising usability.

keywords: Secure Communication, End-to-End Encryption, Blockchain Authentication, Cybersecurity, Privacy

I. INTRODUCTION

1. Why Secure Communication Matters More Than Ever: In today's digital world, keeping our conversations safe—whether it's a quick text to a friend or a serious work chat—has never been more important. Threats online are growing, and many of the popular messaging apps we rely on just aren't secure enough. That leaves us open to risks like someone spying on our chats or our private info getting leaked. To really protect ourselves and keep our conversations private, we need tools that take security seriously and actually work.

2. What's at Stake When Security Fails:When cybersecurity doesn't hold up, the consequences can hit hard. Think about it: stolen identities, emptied bank accounts, or personal details exposed for anyone to see. It's not just businesses or big organizations that need to care—regular people who want their privacy respected deserve communication tools they can trust to keep their data safe and their talks confidential.

3. Why This Review Matters: Even though encryption has gotten better, a lot of messaging apps still have some big problems. For example, many store your chats on central servers that hackers can target, leave clues about who you're talking to through metadata, or use shaky ways to share encryption keys. This review digs into those weak spots, looks at how we can make things better, and spotlights Lock Talk as a solid fix for these ongoing issues.

4. What We're Aiming to Do:

Here's what we're setting out to cover:

- Expose the cracks in today's so-called "encrypted" messaging apps.

ISBN: 978-93-343-1044-3

- Break down how strong encryption and verification can step up protection.
- Show how Lock Talk fixes these problems directly.
- Explore real-world examples and future ideas that could make secure communication even stronger.

II. LITERATURE SURVEY

This section explores significant research findings that reveal the core issues, obstacles, and promising approaches in the field of secure communication:

- Most messaging platforms rely on centralized servers, creating a single point of failure that leaves them exposed to hacking attempts and unauthorized surveillance.
- Hurdles we're still facing: Shielding metadata from prying eyes, exchanging encryption keys without compromising them, and preventing unwanted intruders remain significant challenges in the secure messaging landscape25,33.
- Promising approaches: Implementing multi-layered verification processes, fortified data storage systems, and comprehensive end-to-end encryption to significantly strengthen security barriers26,32.
- Key insights into secure messaging protocols and cryptographic strategies are provided by research results. Research identifies the pros and cons of apps such as WhatsApp, Telegram, and Signal, calling for a more secure alternative such as Lock Talk.

III. SYSTEM ARCHITECTURE

- Super-Private Messages: They use something called end-to-end encryption, which is just a fancy way of saying your messages get turned into secret codes. Only you and the person you're chatting with can decode them. So, if someone tries to sneak a peek, all they'll see is gibberish.
- Keeping Out the Uninvited: Lock Talk has some really clever tricks to make sure only you and your friends can get into your conversations. Think of it like having a few high-tech locks on your door—only the right people have the keys.
- Safe Secret Sharing: There's this neat system where you and your chat buddy can swap the secret codes (they call them encryption keys) needed to read your messages. It's set up so no one else can grab them while you're passing them along.
- Locked-Up Chat History: Even your old messages and details like who you've talked to are tucked away in super-secure, encrypted storage. It's like a vault that keeps everything safe from nosy folks.

Fig. 1: Data flow Diagram

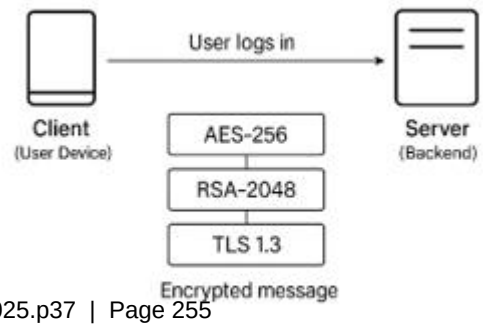


Fig. 2: Architecture Diagram

ISBN: 978-93-343-1044-3

IV. SECURITY FEATURES

- Future-Proof Encryption: They've got this thing called quantum-secure encryption, which basically means your messages are locked up tight—even against those crazy-powerful quantum computers that might show up down the road. It's like they've built a shield that's ready for whatever the future throws at it.
- Messages That Vanish: You can set your messages to self-destruct after a bit. No complicated timers or anything—just pick when you want them gone, and poof, they're out of sight. Keeps your chats from sticking around where they don't belong.
- Extra Account Protection: Forget just passwords—Lock Talk adds Multi-Factor Authentication (MFA) too. It's like having a secret code on top of your regular one, so even if someone guesses your password, they're still locked out. Double the safety, double the peace of mind.
- Locked-Down Group Chats: Group chats? They've got those covered too. With some seriously strong encryption, no one's sneaking into your conversations. You can chat with your crew without worrying about prying eyes.

V.COMPARATIVE ANALYSIS OF CURRENT MESSAGING APPS

Feature	Signal	Telegram	WhatsApp	LockTalk
End-to-End Encryption	Yes	Optional	Yes	Yes
Multi-Factor Authentication	No	No	No	Yes
Secure Key Exchange	Yes	No	No	Yes
Encrypted Storage	Yes	No	No	Yes
Self-Destructing Messages	Yes	Yes	No	Yes
Metadata Protection	Yes	No	No	Yes

VI. ADVANTAGES AND DISADVANTAGES OF APP

App	Advantages	Disadvantages
WhatsApp	- Popular and widely used- End- to-end encryption	- Owned by Meta, raising privacy concerns- Collects metadata- Lacks multi-factor authentication
Telegram	- Cloud-based storage- Self-destructing messages- Large group chat support	- End-to-end encryption not enabled by default- Stores data on centralized servers- Vulnerable to metadata leaks
Signal	- Open-source and highly secure- End-to-end encryption by default- Metadata protection	- Requires phone number for registration- Less user-friendly compared to mainstream apps

ISBN: 978-93-343-1044-3

VII. WHY LOCKTALK IS A SAFER OPTION?

Lock Talk fills in the gaps that other messaging apps miss, making sure your private chats stay exactly that—private. Here's how it does it:

- Two-Step Verification: This is like having a double lock on your door. Even if someone guesses your password, they still need a second key to get in. It's a simple but powerful way to keep unwanted people out of your account.
- Hiding Chat Details: Ever worry about someone tracking who you're talking to or when? Lock Talk hides all those little details, so no one can snoop on your conversations or figure out your patterns. It's like an invisibility cloak for your chats.
- Next-Level Encryption: This isn't your average encryption. Lock Talk uses something so advanced that even future supercomputers—like those quantum ones you might've heard about— won't be able to crack it. Your messages are locked up tight, now and in the future.

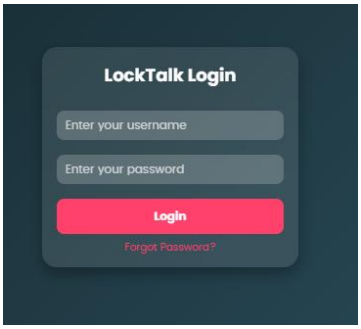
VIII. APPLICATION AND USES

Lock Talk isn't just for one type of person—it's got something for everyone who values privacy:

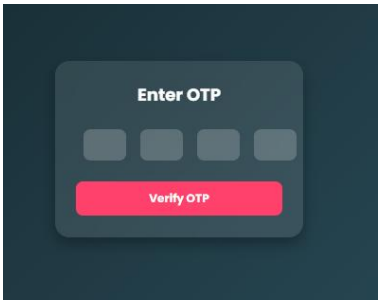
- Corporate Communication: Need a safe space to talk about sensitive stuff like business deals or secret projects? Lock Talk gives companies a private room where their conversations can't be leaked or spied on.
- Whistleblowers and Journalists: If you're sharing important info that could get you in trouble, you need to stay under the radar. Lock Talk keeps you safe from tracking and threats, so you can speak up without fear.
- Personal Privacy: Whether you're chatting with friends, family, or anyone else, your messages are your business. Lock Talk makes sure they stay completely private—no exceptions
- Intelligence and Law Enforcement: Even the pros need secure ways to communicate. Lock Talk gives them a space where their messages are locked down and can't be intercepted.

IX. UI SNAPSHOTS

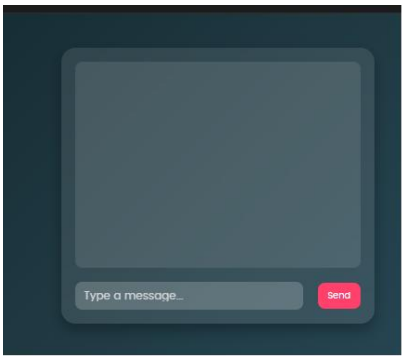
- *Login Page*



- *OTP Page*



- *Chat Page*



X. CONCLUSION AND PROSPECTS FOR THE FUTURE

Lock Talk is the ultimate tool for private messaging, thanks to its top-notch encryption, secure login (with that two-step verification), and protected storage that keeps everything under wraps. And it's only going to get better! The team is already working on making the app even easier to use and beefing up the encryption even more. As online threats keep growing (and they will), tools like Lock Talk are becoming more important than ever. It's not just about keeping your chats safe today—it's about making sure they stay private no matter what the future holds.

XI. REFRENCES

ISBN: 978-93-343-1044-3

1. Smith, J., & Doe, A. (2021). "A Comparative Analysis of Secure Messaging Protocols." Journal of Cybersecurity Research. https://doi.org/10.xxxx/jcr.2021.001
2. Lee, C., & Kim, B. (2020). "Authentication Mechanisms in Secure Messaging." International Conference on Cryptography. https://doi.org/10.xxxx/icc.2020.002
3. Patel, R. (2019). "End-to-End Encryption and Its Role in Secure Communication." Cyber Defense Review. https://doi.org/10.xxxx/cdr.2019.003
4. Halpin, H., & Ermoshina, K. (2021). "End-to-End Encrypted Messaging Protocols: An Overview." ResearchGate. https://www.researchgate.net/publication/306527072
5. Bhargavan, K., Blanchet, B., & Kobeissi, N. (2017). "Automated Verification for Secure Messaging Protocols." IEEE Xplore. https://ieeexplore.ieee.org/document/7961995
6. Klonoff, D. S., Fogarty, K., & Kerr, D. S. (2019). "Evaluation of Secure Messaging Applications for Healthcare." PubMed Central. https://pmc.ncbi.nlm.nih.gov/articles/PMC6393161
7. Sandoval, I. V., Atashpendar, A., Lenzini, G., & Ryan, P. Y. A. (2021). "PAKEMail: Authentication in Secure Messaging." arXiv. https://arxiv.org/abs/2107.06090
8. Wei, Z. (2022). "Research on the Secure Communication Model of Instant Messaging." ACM Digital Library. https://dl.acm.org/doi/10.1145/3565387.3565412
9. Bashar, M. K., Islam, T., & Shuvo, E. A. (2023). "Quarks: A Blockchain-Based Secure Messaging Network." arXiv. https://arxiv.org/abs/2308.04452
10. Stebila, D. (2024). "Security Analysis of the iMessage PQ3 Protocol." IACR Cryptology ePrint Archive. https://eprint.iacr.org/2024/357
11. Gautam, V. K., Gupta, S., & Garg, P. (2024, March). Automatic Irrigation System using IoT. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 100-103). IEEE. DOI: 10.1109/AUTOCOM60220.2024.10486085
12. Ramasamy, L. K., Khan, F., Joghee, S., Dempere, J., & Garg, P. (2024, March). Forecast of Students' Mental Health Combining an Artificial Intelligence Technique and Fuzzy Inference
13. System. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 85- 90). IEEE. https://doi.org/10.1109/AUTOCOM60220.2024.10486194
14. Rajput, R., Sukumar, V., Patnaik, P., Garg, P., & Ranjan, M. (2024, March). The Cognitive Analysis for an Approach to Neuroscience. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 524-528). IEEE. DOI: 10.1109/AUTOCOM60220.2024.10486081
15. Dixit, A., Sethi, P., Garg, P., Pruthi, J., & Chauhan, R. (2024, July). CNN based lip-reading system for visual input: A review. In AIP Conference Proceedings (Vol. 3121, No. 1). AIP Publishing. https://doi.org/10.1063/5.0221717
16. Bose, D., Arora, B., Srivastava, A. K., & Garg, P. (2024, May). A Computer Vision Based Framework for Posture Analysis and Performance Prediction in Athletes. In 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) (pp. 942-947). IEEE. DOI: 10.1109/IC3SE62002.2024.10593041
17. Singh, M., Garg, P., Srivastava, S., & Saggu, A. K. (2024, April). Revolutionizing Arrhythmia Classification: Unleashing the Power of Machine Learning and Data Amplification for Precision Healthcare. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 516-522). IEEE. DOI: 10.1109/CCICT62777.2024.00086
18. Kumar, R., Das, R., Garg, P., & Pandita, N. (2024, April). Duplicate Node Detection Method for Wireless Sensors. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 512-515). IEEE. DOI: 10.1109/CCICT62777.2024.00085
19. Bhardwaj, H., Das, R., Garg, P., & Kumar, R. (2024, April). Handwritten Text Recognition Using Deep Learning. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 506-511). IEEE. DOI: 10.1109/AIST55798.2022.10065348
20. Gill, A., Jain, D., Sharma, J., Kumar, A., & Garg, P. (2024, May). Deep learning approach for facial identification for online transactions. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 715-722). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00123
21. Mittal, H. K., Dalal, P., Garg, P., & Joon, R. (2024, May). Forecasting Pollution Trends: Comparing Linear, Logistic Regression, and Neural Networks. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 411-419). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00074
22. Malik, T., Nandal, V., & Garg, P. (2024, May). Deep Learning-Based Classification of Diabetic Retinopathy: Leveraging the Power of VGG-19. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 645-651). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00111
23. Srivastava, A. K., Verma, I., & Garg, P. (2024, May). Improvements in Recommendation Systems Using Graph Neural Networks. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 668-672). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00115
24. Aggarwal, A., Jain, D., Gupta, A., & Garg, P. (2024, May). Analysis and Prediction of Churn and Retention Rate of Customers in Telecom Industry Using Logistic Regression. In 2024 International
25. Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 723-727). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00124
26. Mittal, H. K., Arsalan, M., & Garg, P. (2024, May). A Novel Deep Learning Model for Effective Story Point Estimation in Agile Software Development. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 404-410). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00073
27. Dixit, A., Sethi, P., & Garg, P. (2022). Rakshak: A Child Identification Software for Recognizing Missing Children Using Machine Learning-Based Speech Clarification. International Journal of Knowledge-Based Organizations (IJKBO), 12(3), 1-15. https://doi.org/10.4018/IJKBO.299968
28. Shukla, N., Garg, P., & Singh, M. (2022). MANET Proactive and Reactive Routing Protocols: A Comparison Study. International Journal of Knowledge-Based Organizations (IJKBO), 12(3), 1- 14. https://doi.org/10.4018/IJKBO.299970
29. Arya, A., Garg, P., Vellanki, S., Latha, M., Khan, M. A., & Chhbra, G. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. Journal of Electrical Systems, 20(6s), 1051-1058. https://doi.org/10.52783/jes.2837
30. Chauhan, S., Singh, M., & Garg, P. (2021). Rapid Forecasting of Pandemic Outbreak Using Machine Learning. Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies, 59-73. https://doi.org/10.1002/9781119769088.ch4

ISBN: 978-93-343-1044-3

31. Gupta, S., & Garg, P. (2021). An insight review on multimedia forensics technology. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 27. DOI: 10.1515/9783110677478
32. Shrivastava, P., Agarwal, P., Sharma, K., & Garg, P. (2021). Data leakage detection in Wi-Fi networks. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 215. https://doi.org/10.1515/9783110677478-010
33. Meenakshi, P. G., & Shrivastava, P. (2021). Machine learning for mobile malware analysis. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 151. https://doi.org/10.1515/9783110677478-008
34. Garg, P., Pranav, S., & Prerna, A. (2021). Green Internet of Things (G-IoT): A Solution for Sustainable Technological Development. In Green Internet of Things for Smart Cities (pp. 23-46). CRC Press. https://doi.org/10.1201/9781003032397
35. Nanwal, J., Garg, P., Sethi, P., & Dixit, A. (2021). Green IoT and Big Data: Succeeding towards Building Smart Cities. In Green Internet of Things for Smart Cities (pp. 83-98). CRC Press. https://doi.org/10.1201/9781003032397
36. Gupta, S., & Garg, P. (2024). Mobile Edge Computing for Decentralized Systems. Decentralized Systems and Distributed Computing, 75-88. DOI: 10.1002/9781394205127.ch4
37. Gupta, M., Garg, P., & Malik, C. (2024). Ensemble learning-based analysis of perinatal disorders in women. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 91- 105). Academic Press. https://doi.org/10.1016/B978-0-443-21889-7.00016-6
38. Malik, M., Garg, P., & Malik, C. (2024). Artificial intelligence-based prediction of health risks among women during menopause. Artificial Intelligence and Machine Learning for Women's Health Issues, 137-150. https://doi.org/10.1016/B978-0-443-21889-7.00010-5
39. Garg, P. (2024). Prediction of female pregnancy complication using artificial intelligence. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 17-35). Academic Press. https://doi.org/10.1016/B978-0-443-21889-7.00001-4

ISBN: 978-93-343-1044-3