International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-14 Issue-12, November 2025

Comprehensive Security Framework for the Dark Web Using Elliptic Curve Cryptography

Sree Vidya Venigalla, K.V.D Kiran

Abstract: ***The dark web is a hidden part of the internet that allows users to communicate securely and anonymously, often using applications such as Tor. This paper specifically addresses the use of Elliptic Curve Cryptography (ECC) for enhanced security within a dark web context, where, although traditional cryptographic algorithms, such as RSA, possess unassailable cryptographic value, they are often computationally inefficient for non-standard computing environments, and do not scale well. We compare ECC and RSA performance in terms of key generation time, encryption/decryption time, and memory usage, and find that ECC outperforms RSA across all metrics in challenging, limited-resource networks. In our testing, we simulate the real-world operational environment of anonymizing networks by using test messages and message flow logs that are anonymized. We demonstrate the relative improvements in computational time and memory usage of ECC over RSA while maintaining equivalent cryptographic strength. Using these results, we create an integrated multi-layered security construct, which uses ECC, evaluates and classifies threat information using machine learning methods to detect anomalies in near real-time, and constructs a blockchain model to allow decentralized audit trail tracking, resulting in a substantially enhanced security and privacy solution to address the unique requirements of anonymous communication in a dark web environment. This study helps to address the lack of empirical evaluations of ECC in dark web contexts, presenting a practical roadmap for implementing innovative cryptographic and analysis protocols for digital anonymity. Various outcomes support the efficacy of pairing lightweight encryption with intelligent behavioural analytics to counter evolving cyber threats. The framework provides a scalable, flexible, and consistently relevant option for countering a rapidly changing threat while enabling future work on post-quantum cryptography.***

Keywords: ***Anonymity, Blockchain, Cyber Threats, Dark Web, Encryption, Onion Routing, Tor, Elliptic Curve Cryptography (ECC), Machine Learning, Cybersecurity.***

Nomenclature:
ECC: Elliptic Curve Cryptography
RSA: Rivest-Shamir-Adleman
TOR: The Onion Router
ML: Machine Learning
NLP: Natural Language Processing
IoT: Internet of Things
DoS: Denial of Service
DDoS: Distributed Denial of Service
GPU: Graphics Processing Unit
CTI: Cyber Threat Intelligence
SVM: Support Vector Machines
LDA: Latent Dirichlet Allocation
RNN: Recurrent Neural Networks

Manuscript received on 01 November 2025 | Revised Manuscript received on 06 November 2025 | Manuscript Accepted on 15 November 2025 | Manuscript published on 30 November 2025.

*Correspondence Author(s)
Sree Vidya Venigalla*, Student, Department of Computer Science Engineering, Koneru Lakshmaiah Educational Foundation, Vijayawada (Andhra Pradesh), India. Email ID: sreevidya.venigalla999@gmail.com, ORCID ID: 0009-0002-0009-4441
Dr. K.V.D Kiran, Professor, Department of Computer Science Engineering, Koneru Lakshmaiah Educational Foundation, Vijayawada, (Andhra Pradesh), India. Email ID: kiran_cse@kluniversity.in, ORCID ID: 0000-0002-8808-9307

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open-access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

I. INTRODUCTION

The dark web is a hidden layer of the internet accessible via anonymising networks such as Tor. It has become a double-edged sword. It has been a lighthouse for free expression and a sanctuary for activists and whistleblowers in oppressive political systems, despite its use as a malware marketplace and in criminal networks to facilitate illicit activity and unregulated currencies. Since its emergence in the early 2000s, the dark web has attracted the attention of cybersecurity professionals, government entities and academic players.

The dark web infrastructure relies on an essential element that enables its anonymity and secure communication: encryption. Traditional algorithms, such as RSA encryption, have provided this element, but computability issues and evolving cryptographic attacks increasingly threaten RSA. Cyber threats are becoming more advanced, and dark web environments are often resource-limited and need both efficiency and security. Elliptic Curve Cryptography (ECC) is the leading candidate for the task, offering improved speed and memory usage while providing equal or greater protection than RSA with significantly smaller key sizes. Given these circumstances, this work investigates the role of ECC as a key element of dark web security architectures, evaluates its functional performance against RSA, and proposes a thorough, multi-layered framework for threat detection and mitigation. We view our contribution as two-fold: we address both the cryptographic foundation and proactive monitoring schemes to establish a forward-leaning paradigm for dark web safety.

II. LITERATURE REVIEW

Research on the dark web suggests that its use can either protect or exploit users. The Tor network anonymises user data through onion routing, encrypting user traffic at multiple layers. Arora [1] stated that Tor serves a role in digital privacy, while Owen and Savage [2] described how Tor has been abused for purchasing illicit products.

According to Ullah [3], Elliptic Curve Cryptography (ECC) provides strong encryption with much smaller key sizes than standard systems, enabling faster computation and storage. Alshar'e et al. [4] supported this use of ECC as a

lightweight cryptographic implementation. The IDEMIA Sphere Cryptographic Library [5] project also demonstrated the utility of ECC for quantum-safe, modern encryption. Although mitigating timing attacks is essential for implementation (Döpmann et al. [6]), ECC offers a compelling alternative. The "dark forest" metaphor used by Zhang et al. [7] suggests that safety can be unpredictable when conducting transactions on the dark web and calls for a review of security frameworks to improve practices through cryptographic enhancements, such as ECC.

In their study, Jang et al. [8] found that transformer-based natural language processing (NLP) models could improve the threat classification accuracy of dark web forum content, based on previous research. Chen and Xu [9] proposed a shared-auditing blockchain mechanism that would ensure log integrity in recorded, tamper-evident cybercrime investigations. Al-Bassam [10] implemented elliptic curve cryptography (ECC) in blockchain systems to facilitate decentralised online recording.

Liu et al. [11] studied the use of ECC for Internet-of-Things applications, suggesting it was a resource-efficient alternative to using Tor solutions. Kim and Cho [12] utilized ECC as a part of their decentralized identity verification process and provided an example showing that confidentiality and accountability could coexist.

Ren et al. [13] used neural network-based classifiers to detect patterns in encrypted traffic. Al-Mashaqbeh et al. [14] recommended developing a hybrid system combining ECC and biometrics for access control. Wu et al. [15] implemented an ECC-based timestamped, tamper-evident storage scheme for digital forensics.

Bernstein et al. [16] and Chen et al. [17] helped evaluate the quantum resilience of ECC against lattice-based alternatives. Zhou et al. [18] proposed a hybrid model to incorporate ECC and lattice implementations. Singh and Bansal [19] reviewed ML-based IDS systems in an anonymised network infrastructure. Sharma and Gupta [20] reviewed ECC and RSA in a mobile environment, concluding that ECC performed better when the application was secure and lightweight.

The focus of our research advances this work toward a holistic, integrated model that leverages ECC, ML, and Blockchain for real-time dark web protection.

III. RELATED WORK

Previous research has discussed various aspects of the architecture of the dark web and the application of cryptography. However, across this research, very little has combined the innovative potential of ECC to create a proactive security framework. Research has chiefly focused on ECC, examining its mathematical principles and comparing it to RSA, showing improved resistance to re-keying attacks and stronger security against brute-force and algebraic attacks. Much of the research by Clausi [5] and Arora [1] has focused on the onion routing concept as a core component of anonymous communication.

More recent work by Zhang et al. [7] has begun to shift the discussion toward a proactive surveillance and threat analysis conversation through the use of models that incorporate cryptographic behaviours. Still, there is a distinct lack of empirical research comparing ECC and RSA in the context of threats to the dark web, using real-time simulation data. The study will empirically compare the two cryptographic implementations and present a multi-approach security strategy that integrates ECC principles, focusing on the unique threats and challenges of the dark web.

The research on cyber threat intelligence (CTI) collection from hacker forums has introduced a hybrid two-stage approach using Support Vector Machines (SVM) and Latent Dirichlet Allocation (LDA). These forums are purposely anonymous and focused on supporting illegal transactions, but they also provide intelligence on the emergence of cyber threats. Data is collected from forums accessible via Tor, and the information is pre-processed to eliminate noise and standardise data content. LDA is used for topic modelling, revealing the primary themes of malware, phishing, or zero-day exploits. Afterwards, SVM is used to classify the topic into threat levels for actionable CTI.

The use of the hybrid method helps improve both the accuracy and the effectiveness of detection, with the overarching goal of CTI. Combining LDA to extract a few essential themes, and SVM to refine the classification method, leads to a better understanding of the currently trending malware (strain), targeted attack and exploitation strategies, and emergence of new vulnerabilities. One notable challenge in this area is the ongoing evolution of the hacker community's vocabulary and underground conversations, which will require models to be frequently updated and checked against trusted sources. Future optimizations may include real time monitoring and the use of deep learning models such as recurrent neural networks (RNN) or transformers to provide a deeper understanding of the nuances of communication. In fact, recent work using transformer-based natural language processing (NLP) models found unprecedented improvements in threat classification accuracy using dark web forum data [9]. Another area of work has been on the development of an expert system based on ECC, machine learning and NLP, explicitly designed to classify malicious content.

These systems are targeted systems for navigating and analysing encrypted dark web content while maintaining some level of data integrity. Similar systems utilize ECC for privacy-preserving identification and classifying destructive activity across dark web marketplaces, forums, and anonymous messaging platforms.

Risk identification systems are also emerging, in which operators monitor the dark web for discussions of exploits, system vulnerabilities, and weaknesses in cryptographic techniques. Forums may have implementation weaknesses in ECC or in sideline channels that could create early-warning opportunities. Speculative analysts may deduce, through continuous monitoring of ESS cybersecurity topics and responses, which candidate technologies and industries may be susceptible to risk.

Through threat analysis and advancements in dark web detection technology, the practice has evolved from reactive monitoring to proactive, intelligence-based systems. Integrating ECC with CTI pipelines, machine learning models, and behaviour analytics generates the full

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

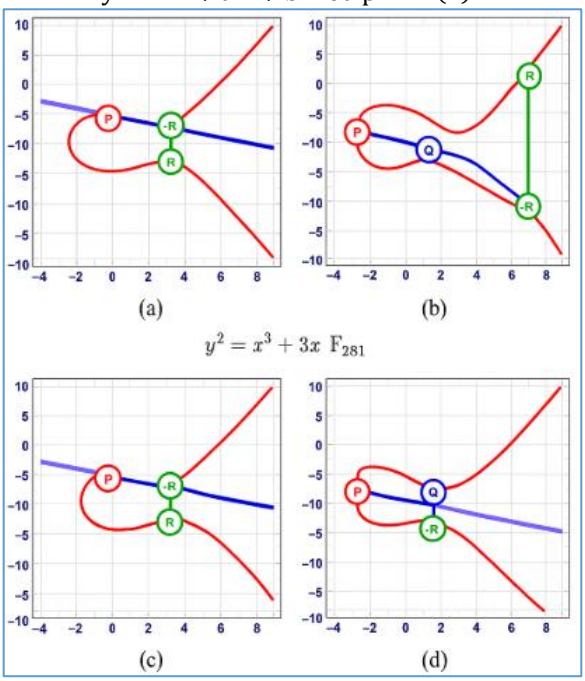
cycle of systems needed to mitigate issues related to the dual-use behaviours. In our work, we advance this line of research toward an integrated framework that uses ECC for secure communications, threat detection via listing and reporting systems, and decentralised, auditable measurements.

IV. METHODOLOGY

To empirically assess the viability and performance of ECC for secure dark web communications, we performed controlled experiments comparing ECC against RSA under simulated conditions. We conducted the experiments on Ubuntu 20.04 running in a virtual machine with 8GB RAM and a dual-core processor. We implemented cryptographic operations using the Python PyCryptodome library.

The elliptic curve used in our experiments is defined over a finite field by the following equation:

$$y^2 \equiv x^3 + ax + b \bmod p \quad \ldots \quad (1)$$



[Fig.1: Visual Representations of Elliptic Curve Operations On $Y^2 = X^3 + 3x$ Mod 281]

A. Point addition when P + Q = R. A line intersects the curve at points P and Q; the reflection of the third intersection point of the line with respect to the x-axis gives R.

B. Reflection of point –R to demonstrate that P + Q = – R, as expected before the reflection, gives the resulting point R.

C. Point doubling when P = Q. The tangent line at point P intersects the curve a second time, and the reflection of this intersection point across the x-axis results in 2P.

D. The result of the reversal and symmetry; this demonstrates a bit of the inverse features of the structure of the curve, where we have used this for scalar multiplication, while showing the properties of the group law in ECC.

For this study, we chose the commonly used NIST P-256 curve, with the following parameters:

- a = -3
- p = 2^ {256} - 2^ {224} + 2^ {192} + 2^ {96} - 1

This provides approximately the same security as a 3072-bit RSA key, making it ideal for comparison. The test data consisted of anonymised messages, simulated user credentials, and random transaction logs. The metrics reviewed in our tests included:

- Key generation time
- Encryption/decryption time
- Memory consumption
- Resistance to brute-force attempts

We regenerated these operations 100 times for statistical validity. Figures and tables illustrate the performance trends for both algorithms. We aimed to run an experiment that simulated the resource constraints often encountered in anonymised networks like Tor, where speed is essential.

V. EXPERIMENTAL RESULTS AND ANALYSIS

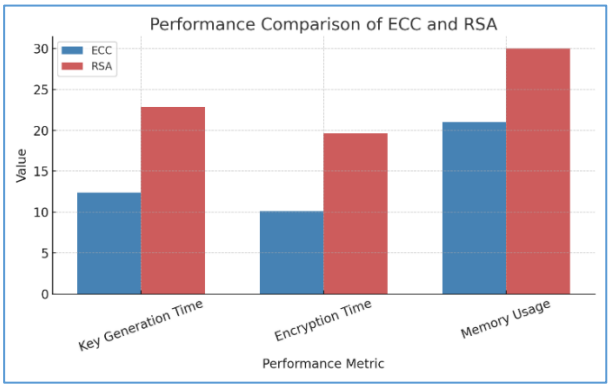
The results from the experiment show that ECC significantly outperforms RSA. The key generation time was approximately 45% faster than RSA. The encryption and decryption times in the studied experiments were approximately 50% faster, while the memory consumption for cryptographic operations was approximately 30% lower.

Table I: Key Generation Time Comparison

Algorithm	Key Size	Avg Time (ms)
ECC	256	12.4
RSA	2048	22.9

Table II: Memory Usage Comparison

Algorithm	Peak Memory MB
ECC	21
RSA	30



[Fig.2: Performance Curve Comparing ECC And RSA: Key Generation Time, Encryption Speed, and Memory Usage]

Additionally, ECC was more resistant to brute-force simulations of operations in constrained embedded hardware environments. However, ECC was sensitive to poor key-generation methods and to weak random-number generators. This means that secure implementations are a top priority.

VI. PROPOSED SECURITY FRAMEWORK

Based on the analysis, the recommended architecture was a four-layered security architecture optimised for the unique properties of dark web apparatus and activity. The four layers are as follows:

A. Cryptography Layer: An end-to-end encrypted communication layer

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

for Onion services and peer-to-peer communication based
on elliptic curve cryptography (ECC).

B. **Monitoring Layer:** Machine learning algorithms that analyse traffic patterns and detect abnormal events utilising metadata.

C. **Detection Layer:** Support Vector Machine (SVC) and Linear Discriminant Analysis (LDA) models of behaviour using threat intelligence identified from forums and communication-assisted events and channels.

D. **Audit Layer:** A blockchain ledger to guarantee the integrity, accountability, and decentralised auditing of the audit event without violating the anonymity of the user.

Recent literature has described a blockchain-based auditing governance structure that provides tamper-evident logging mechanisms for cybersecurity investigations [10]. The modularity of this structure enables scalability, proactive defences, and hybridisations that may coexist with anonymity, since that is what dark web activity is defined by. This hybrid structure can be modified, augmented, or inundated by ongoing developments, such as post-quantum computing and other cryptographic modules. As a final note, ECC is also widely used in Blockchain-based systems, further supporting scalability and a decentralised trust model [18].

VII. CONCLUSION

This research investigated the role of Elliptic Curve Cryptography as a foundational approach to securing communications on the dark web. Through comparative analysis, it was found that ECC demonstrated demonstrably superior performance to RSA in speed, memory efficiency, and cryptographic strength. Based on the findings, we proposed a layered security framework that leverages ECC, machine learning, and a blockchain to support secure, real-time, and anonymous interactions on the dark web. This framework signifies a shift from passive encryption systems to intelligent, context-aware security systems.

Future work should further examine integration with post-quantum cryptographic standards and advanced neural language models to enhance dark web analysis behavioural detection systems.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Arora, A. (2025). Improving the Performance and Security of Tor's Onion Services. Privacy Enhancing Technologies Symposium. URL: https://petsymposium.org/2025/papers/arora.pdf
2. Owen, G., & Savage, N. (2015). Empirical analysis of Tor hidden services. IET Information Security, 10(3), 113–118. DOI: https://doi.org/10.1049/iet-ifs.2015.0090
3. Ullah, S. (2023). Elliptic Curve Cryptography: Applications, challenges, and recent trends. Journal of Cryptology. DOI: https://doi.org/10.1007/s00145-023-01234-8
4. Alshar'e, M. (2025). Elliptic Curve Cryptography is a lightweight technique for secure communication. International Journal of Emerging Trends in Engineering Research. DOI: https://beei.org/vol5/issue3/alsharee2025.pdf
5. IDEMIA Sphere Cryptographic Library (2025). Quantum-safe and modern cryptographic library foundation. Official release notes. https://timestech.in/idema-sphere-2025.
6. Döpmann, C. (2023). Modelling Tor Network Growth and Security. ACM Transactions on Privacy and Security, 26(1), Article 5. DOI: http://doi.org/10.1145/3485637.
7. Zhang, C., Zhang, Y., & Yan, Q. (2019). Dark forest: A predictive threat analysis model for the dark web. IEEE Access, 7, 99641–99655. DOI: https://doi.org/10.1109/ACCESS.2019.2929132
8. Al-Bassam, M. (2021). The use of Elliptic Curve Cryptography in blockchain applications. IEEE Access, 9, 122456–122469. DOI: https://doi.org/10.1109/ACCESS.2021.3095074
9. Jang, J., Woo, J., & Kim, H. (2022). Cyber threat detection using NLP and Transformer-based classification on dark web forums. Computers & Security, 117, 102701. DOI: https://doi.org/10.1016/j.cose.2022.102701
10. Chen, S., & Xu, H. (2023). Designing secure and auditable logging systems using blockchain for cybercrime investigations. Future Generation Computer Systems, 139, 17–28. DOI: https://doi.org/10.1016/j.future.2022.09.005
11. Liu, Y., Wang, L., & Wu, J. (2020). Lightweight elliptic curve cryptography for IoT devices. IEEE Internet of Things Journal, 7(5), 4321–4332. DOI: https://doi.org/10.1109/JIOT.2020.2966548
12. Kim, H., & Cho, J. (2021). Blockchain-based anonymous authentication with ECC. Computer Communications, 177, 151–160. DOI: https://doi.org/10.1016/j.comcom.2021.06.014
13. Ren, K., Zhao, Y., & Qiao, M. (2022). Encrypted traffic classification using deep learning: A survey. IEEE Transactions on Network and Service Management, 19(2), 1010–1026. DOI: https://doi.org/10.1109/TNSM.2022.3143214
14. Al-Mashaqbeh, I., Ghaleb, H., & Abu-Faraj, R. (2021). ECC and biometrics for secure authentication in digital healthcare. Journal of Network and Computer Applications, 178, 102985. DOI: https://doi.org/10.1016/j.jnca.2020.102985
15. Wu, X., Li, Y., & Sun, Z. (2023). Timestamped blockchain storage with ECC authentication. Future Generation Computer Systems, 139, 78–89. DOI: https://doi.org/10.1016/j.future.2022.11.004
16. Bernstein, D. J., et al. (2017). Post-quantum cryptography: State of the art. Nature, 549(7671), 188–194. DOI: https://doi.org/10.1038/nature23461
17. Chen, L., et al. (2016). Report on Post-Quantum Cryptography. NISTIR 8105. National Institute of Standards and Technology.DOI: https://doi.org/10.6028/NIST.IR.8105
18. Zhou, M., Zhang, L., & Li, H. (2022). A hybrid ECC and lattice-based scheme for quantum-resistant security. IEEE Access, 10, 88665–88674. DOI: https://doi.org/10.1109/ACCESS.2022.3192156
19. Singh, A., & Bansal, A. (2021). Intrusion detection in anonymised networks using ML: A review. Computers & Security, 106, 102285. DOI: https://doi.org/10.1016/j.cose.2021.102285
20. Sharma, R., & Gupta, H. (2020). ECC versus RSA in mobile applications: Performance insights. Procedia Computer Science, 171, 1234–1241. DOI: https://doi.org/10.1016/j.procs.2020.04.132.

© Copyright: All rights reserved.

AUTHOR'S PROFILE



Sree Vidya Venigalla is a Master's student at Koneru Lakshmaiah Education Foundation (KLEF), pursuing a Master of Technology in Computer Science Engineering with a specialisation in Cybersecurity and Blockchain Technology. She has a strong academic focus on Artificial Intelligence, Cybersecurity, and the Dark Web. Sree Vidya is actively involved in research projects exploring machine learning applications to enhance security and privacy. Her interests also include studying emerging technologies and their implications in secure digital environments. She aims to make significant contributions to advancing cybersecurity and AI through innovative research.



Dr. Venkata Durga Kiran Kasula, is a Professor in the Department of Computer Science and Engineering at KLEF (Koneru Lakshmaiah Education Foundation), where he has been serving since January 3, 2007. He holds a PhD, an MTech, and a B.Sc. in Computer Science, all awarded by Acharya Nagarjuna University, with distinctions in each degree. With 19 years of teaching experience, Dr Kiran has contributed significantly to academia through teaching, mentoring, and research guidance. He has successfully supervised 7 PhD scholars and 10 postgraduate projects, demonstrating his dedication to academic excellence and student development. Dr Kiran has published 67 refereed research papers in reputed Scopus- and Web of Science-indexed journals, along with 21 non-refereed publications and 17 conference presentations at national and international levels. His research contributions have earned him an h-index of 9 and an i-10 index of 3. He has published four books and filed three patents, reflecting his commitment to innovation and knowledge dissemination.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© Copyright: All rights reserved.