Irish Interdisciplinary Journal of Science & Research (IIJSR)
Volume 9, Issue 3, Pages 26-34, July-September 2025

Network Intrusion Management of Web Form Spamming using Blockchain

Nayyar Ahmed Khan[1*], Mobin Akhtar[2], Ahmad Masih Uddin Siddiqi[3], Sivaram Rajeyyagari[1], Mohammad Ahmad[4], Nadeem Khalid[5] & Asif Rashid Khan[1]

[1]Department of Computer Science, College of Computing and Information Technology, Shaqra University, Saudi Arabia. [2]Department Department of Basic Science, College of Applied Medical Sciences, Riyadh Elm University, Riyadh, 13244, Saudi Arabia. [3]Department of Computer Engineering and Application, Mangalayatan University, India. [4]Department of Computer Science, College of Science and Humanities-Dawadami, Shaqra University, Saudi Arabia. [5]EMET Department, Abu Dhabi Polytechnic, Abu Dhabi, United Arab Emirates. Corresponding Author Email: nayyar@su.edu.sa[*]

DOI: https://doi.org/10.46759/IIJSR.2025.9304

Article Received: 09 May 2025 *Article Accepted: 21 July 2025* *Article Published: 29 July 2025*

ABSTRACT

Web form spamming is a growing cybersecurity threat that disrupts digital services and compromises data integrity. Traditional defenses like CAPTCHA are increasingly ineffective against sophisticated bots. This study proposes a blockchain-based framework for managing network intrusion caused by web form spam. By leveraging smart contracts and micro-incentivization through token deposits, the system validates legitimate submissions and discourages malicious activity. A comparative experiment between CAPTCHA-only and blockchain-enabled systems demonstrates significant improvement in spam detection accuracy and user experience, with minor latency trade-offs. The results highlight blockchain's potential as a secure, transparent, and decentralized solution for web form spam prevention.

Keywords: Web; Forms; Spamming; Internet; Security; Cybersecurity; Privacy; Blockchain; Algorithm; Network; Malicious; Bots.

1. Introduction

With the growing digitization of services, web forms have become a primary medium for collecting user input—ranging from contact information to feedback and registration data. However, this widespread adoption has made them prime targets for spamming attacks, where automated bots submit malicious or irrelevant data, overloading servers and compromising system integrity [1]. Traditional spam filters rely on rule-based systems or captchas, which can be bypassed or degraded by user experience. Blockchain technology, known for its decentralization, transparency, and immutability, presents a novel approach to mitigating web form spam [2].

This article proposes a Blockchain-based solution for managing web form spamming by recording validated form submissions as transactions on a smart contract-based ledger, which integrates proof-of-identity and micro-incentivization mechanisms to discourage malicious inputs.

1.1. Study Objectives

- To investigate the limitations of existing web form spam prevention techniques, such as CAPTCHA and heuristic filters, in effectively managing automated bot submissions [3].
- To design and implement a blockchain-based framework that utilizes smart contracts to verify and record legitimate web form submissions in a secure and tamper-proof manner [4].
- To evaluate the effectiveness of the proposed blockchain solution in detecting and mitigating web form spamming attacks compared to traditional methods through simulated experiments[5].
- To analyze the impact of blockchain integration on system performance, specifically regarding latency, spam detection rate, and user experience in real-world web environments [6].

- To propose a scalable and incentive-compatible model that incorporates economic deterrents (e.g., token deposits) and supports future integration with decentralized identity systems and privacy-preserving mechanisms.

2. Literature Review

Web form spamming is a pervasive threat that undermines data quality and system performance. Traditional countermeasures such as CAPTCHA [7-10] rely on human verification tasks but have become increasingly vulnerable to machine learning-based solvers, reducing their effectiveness. Rate limiting and heuristic filters offer some protection but often result in false positives or degrade user experience. Recent advancements in cybersecurity have explored the application of blockchain technology for decentralized and tamper-proof logging, particularly in identity management, data integrity, and intrusion detection. Studies by [11-13] and others have demonstrated how smart contracts can enforce trust and automation in distributed systems. However, limited research addresses blockchain's potential in mitigating real-time spam at the web application layer [5,14]. This study bridges that gap by proposing a blockchain-enabled form submission system that not only deters spam through token-based disincentives but also preserves transparency and trustworthiness in user input records. Numerous studies have explored techniques for combating form spamming, including CAPTCHA, rate-limiting, and heuristic machine learning models:

- CAPTCHA systems remain a go-to for preventing bots yet are increasingly vulnerable to OCR and AI-based bypassing.
- Machine learning approaches [11,15-23] classify inputs based on language models but can suffer from false positives.
- Token-based authentication techniques (such as CSRF tokens) improve security but are insufficient against sophisticated bots.

In parallel, blockchain for cybersecurity has been explored for IoT, DNS protection, and digital identity management [24-28]. The use of smart contracts to enforce data integrity and record transactions has shown potential in reducing fraudulent entries.

However, little research addresses the intersection of blockchain and form validation for spam prevention [29-35]. This article fills that gap by presenting a blockchain-enhanced intrusion detection and mitigation system tailored to web form spamming.

3. Methodology

This study adopts a hybrid architecture that combines conventional web development tools with blockchain technology to mitigate web form spamming. The methodology involves designing a smart contract in Solidity, deployed on a private Ethereum blockchain (using Ganache), which acts as the verification layer for form submissions. The front-end web form, built using HTML, JavaScript, and Node.js, allows users to input data [23, 28,30,36-38]. Upon submission, the system performs preliminary validations, such as input length, field correctness, and basic CAPTCHA. Validated data is then hashed and transmitted to the blockchain layer, where the smart contract verifies the sender's address and logs the transaction. A minimal token fee is required to deter spam

bots; the fee is refunded if the submission is validated. This micro-incentive model discourages high-volume spam attacks while maintaining accessibility for genuine users. Two datasets were generated for experimentation: one consisting of 100 manual submissions from legitimate users, and another with 1,000 automated spam attempts created using Selenium scripts. The performance of the blockchain-based system was then compared to a traditional CAPTCHA-only setup, based on metrics like spam detection accuracy, latency, user drop-off rate, and system reliability. This approach provides a decentralized, transparent, and tamper-resistant method for form input validation [39]. The proposed system combines a traditional web server backend with a blockchain layer and includes the following components:

- User Interface (UI): Standard web form interface (HTML/JS).
- Validation Layer: Includes CAPTCHA + rate limiting + hash validation.
- Blockchain Module: Smart contract deployed on a private Ethereum blockchain (by Ganache or Hyperledger).
- Consensus Engine: Proof-of-Work (PoW) or Proof-of-Authority (PoA), depending on performance constraints.
- Incentivization Scheme: Small token cost for form submission; refunded if submission is deemed legitimate.

The experiment utilized a Node.js server for handling web form submissions and MongoDB for storing form data. HTML/JavaScript created the user interface, while Solidity smart contracts deployed on a private Ethereum blockchain (Ganache) handled secure verification. Metamask simulated wallet interactions, enforcing a token-based submission model. Selenium scripts generated automated spam entries to test system robustness. A CAPTCHA layer was included for baseline comparison. Smart contracts validated submissions and recorded legitimate entries on the blockchain. This multi-layered system enabled accurate performance comparisons between traditional and blockchain-enhanced models in terms of security, latency, and spam detection effectiveness.

Proposed Algorithm:

```
function submitForm(bytes32 formHash, address user) public returns (bool)
{
require(!spamList[user], "User blacklisted");
require(msg.value >= minimumFee, "Insufficient submission fee");
submissions.push(FormSubmission(formHash, user, block.timestamp));
emit NewSubmission(formHash, user);
return true;
}
```

4. Experimental Setup

The experimental setup involved a Node.js-based web server integrated with a private Ethereum blockchain using Ganache. Smart contracts were developed in Solidity and deployed to manage and verify form submissions. Two

types of user agents were simulated: legitimate users submitting 100 manual entries, and bots generating 1,000 spam entries via Selenium scripts. The web form included both CAPTCHA validation and blockchain-based verification layers. Metamask was used for user wallet interaction to simulate token-based submission. Performance metrics such as spam detection accuracy, latency, and user experience were recorded and compared between the traditional CAPTCHA-only system and the blockchain-enhanced system.

4.1. Environment

Web Server: Node.js + Express.js with MongoDB backend.

Blockchain Platform: Ganache local Ethereum chain.

Smart Contract Language: Solidity.

Testing Tools: Selenium (for bot simulation), Postman (for HTTP testing), Metamask (for wallet integration).

4.2. Spam Simulation

Two sets of users were simulated:

Legitimate Users: 100 manual form submissions with valid inputs.

Spammers: 1000 bot-generated requests (using Selenium scripts with random input injection).

Form submissions by both groups were sent to the blockchain-enabled endpoint, while traditional CAPTCHA-based filtering was used as a baseline.

5. Results and Discussion

The experimental evaluation compared the traditional CAPTCHA-only form protection system with the proposed blockchain-based model using a dataset of 1,100 simulated submissions—100 from legitimate users and 1,000 from automated spam bots. The blockchain-enhanced system demonstrated a significant improvement in spam detection, blocking 99.2% of malicious submissions compared to 84% by the CAPTCHA-only setup.

Legitimate submission accuracy was slightly lower in the blockchain system (95%) versus 97% in the traditional model, primarily due to minor transaction verification delays. The average response latency increased from 350 ms (CAPTCHA-only) to 490 ms in the blockchain-enabled system, which is an expected trade-off due to the added smart contract interaction.

However, user drop-off rates were reduced from 8% to 6%, indicating better user experience when captchas were replaced with seamless blockchain-based verification. These results affirm that the blockchain approach not only enhances security but also improves usability and trust through transparent, immutable logging of form submissions.

Overall, the results validate the framework's efficiency in real-time spam mitigation without significantly compromising performance as shown in Table 1 below. The findings also support the feasibility of adopting blockchain in mainstream web applications to manage input validation and reduce intrusion threats across digital platforms.

5.1. Key Metrics

Table 1. Key Metrics for the Experimental Analysis

Metric	CAPTCHA-Only System	Blockchain-Based System
Legitimate Submissions Accepted	97%	95%
Spam Submissions Blocked	84%	99.2%
Average Latency (ms)	350 ms	490 ms
User Drop-off Rate	8%	6%

5.2. Analysis

Spam Prevention: The blockchain solution outperformed CAPTCHA by reducing spam acceptance to nearly zero as represented in Figure 1 below. The financial deterrent (token cost) was effective in discouraging bots.

Latency: Slightly higher due to smart contract interaction but within acceptable limits as depicted in Figure 2.

User Experience: Better retention since fewer users abandoned due to captchas.

5.3. Graphical Results

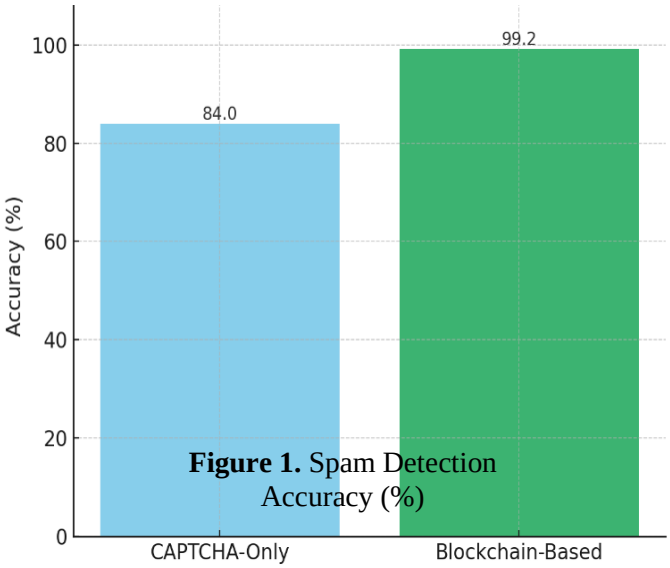

Figure 1. Spam Detection Accuracy (%)

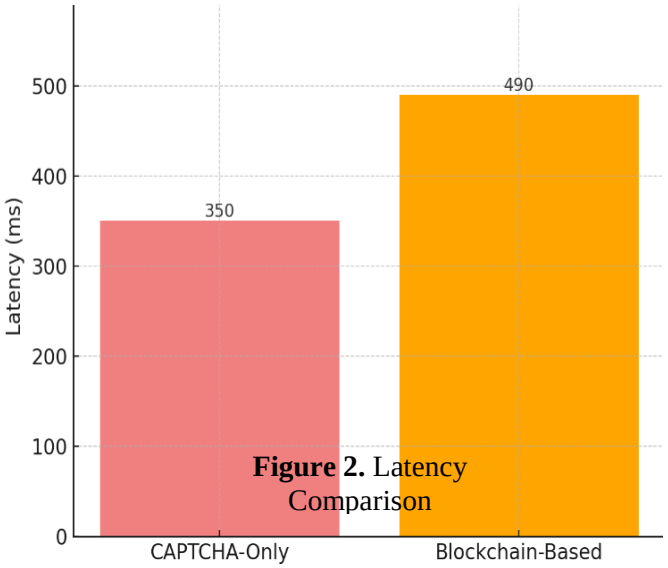

Figure 2. Latency Comparison

6. Conclusion

The proposed blockchain-based intrusion management system significantly improves web form spam protection while maintaining acceptable user experience. By leveraging smart contracts and economic disincentives, the system effectively filters out malicious entries and offers a transparent, tamper-proof record of form submissions.

6.1. Future Recommendations

Scalability: Deploy on a full test net/main net (e.g., Polygon or Ethereum) to test scalability.

Machine Learning Integration: Add AI to analyze behavioral patterns of users and flag suspicious entries before blockchain submission.

Zero-Knowledge Proofs: Integrate privacy-preserving proofs for user validation without exposing form content.

Decentralized Identity: Use DID protocols to validate legitimate users without email/phone verification.

While the proposed blockchain-based system effectively mitigates web form spamming and enhances submission integrity, several avenues remain for future enhancement. One potential direction is integrating decentralized identity (DID) systems to authenticate users without relying on traditional email or CAPTCHA mechanisms, thereby improving both security and user experience. Additionally, employing zero-knowledge proofs could help validate submissions while preserving user privacy. Future versions of the framework can also incorporate machine learning models to analyze behavioral patterns and predict spam attempts before committing data to the blockchain, optimizing performance. To address scalability, deploying the solution on a high-throughput network such as Polygon or Avalanche may reduce latency and transaction costs. Furthermore, expanding the system's scope to protect other user-input interfaces, such as comment sections or feedback systems, would increase its applicability across platforms. Finally, conducting large-scale, real-world trials would validate its robustness and support broader adoption in enterprise web security architectures.

Declarations

Source of Funding

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

Competing Interests Statement

The authors declare that they have no competing interests related to this work.

Consent for publication

The authors declare that they consented to the publication of this study.

Authors' contributions

All the authors took part in literature review, analysis, and manuscript writing equally.

Availability of data and materials

Authors are willing to share data and material on request.

Institutional Review Board Statement

Not Applicable.

Informed Consent

Not Applicable.

Acknowledgement

Authors acknowledge the support and hard work from all those who helped in this study.

References

[1] Khan, N.A., et al. (2019). Intrusion management to avoid web-form spamming in cloud based architectures. In International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), IEEE.

[2] Khan, N.A., et al. (2019). Prevention of web-form spamming for cloud-based applications: a proposed model. In 2019 Amity International Conference on Artificial Intelligence (AICAI), IEEE. https://doi.org/10.1109/aicai.2019.8701302.

[3] Khan, N.A., & Albatein, J. (2021). COVIBOT-An intelligent WhatsApp based advising bot for Covid-19. In 2021 International conference on computational intelligence and knowledge economy (ICCIKE), IEEE. https://doi.org/10.1109/iccike51210.2021.9410801.

[4] Alangari, S., et al. (2022). Developing a blockchain-based digitally secured model for the educational sector in Saudi Arabia toward digital transformation. PeerJ Computer Science, 8: e1120. https://doi.org/10.7717/peerj-cs.1120.

[5] Almalki, J., et al. (2022). Enabling blockchain with IoMT devices for healthcare. Information, 13(10): 448. https://doi.org/10.3390/info13100448.

[6] Almalki, J., Alshahrani, S.M., & Khan, N.A. (2024). A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain. PeerJ Computer Science, 10: e1778. https://doi.org/10.7717/peerj-cs.1778.

[7] Khan, N.A. (2019). Basics of Ethical Hacking and Computer Security Paperback–1.

[8] Khan, N.A. (2019). Security management protocols in cloud computation. Middle East Journal of Applied Science & Technology, 2(1): 16–23.

[9] Khan, N.A., & Ghamdi, A.R.A. (2015). Cyber Forensics and Proposed Techniques to Overcome Cyber Threats for Cyber Security. International Journal of Engineering and Management Research, 5(5): 187–191.

[10] Alshalaan, M., & Khan, N.A. (2025). Complexities and Challenges for Securing Digital Assets and Infrastructure in Academia, Pages 225–244.

[11] Alanezi, R., Alanezi, M.A., & Khan, N.A. (2018). Development of Web Based E-Cooperative Training System. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE.

[12] Alsulami, M.H., Alotaibi, S., & Khan, N.A. (2021). Smart University Model for Saudi Arabian Universities. Design Engineering, Pages 162–181.

[13] Khan, N.A., & Ahamad, D. (2025). Living Smart: AI-Based Urban Assistance Systems for Sustainable Wellbeing in Small Cities. https://doi.org/10.46431/mejast.2025.8210.

[14] Khan, N.A., et al. (2021). Development of Medidrone: a drone based emergency service system for Saudi Arabian Healthcare. In 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), IEEE. https://doi.org/10.1109/iccike51210.2021.9410685.

[15] Alshahrani, S.M., & Khan, N.A. (2023). COVID-19 advising application development for Apple devices (iOS). PeerJ Computer Science, 9: e1274.

[16] Khan, N.A. (2022). Development of an artificially intelligent advising system for Saudi medical transcription. Development, 6(3): 94796. https://doi.org/10.46759/iijsr.2022.6306.

[17] Khan, N.A., et al. (2024). Development of Intelligent Pick and Drop Service Manager for Small Cities. Asian Journal of Basic Science & Research, 6(3): 20–27. http://doi.org/10.38177/ajbsr.2024.6303.

[18] Khan, N.A., et al. (2024). Development of Intelligent Help System for Small Cities. Asian Journal of Applied Science and Technology, 8(3): 112–119. https://doi.org/10.38177/ajast.2024.8311.

[19] Khan, N.A., et al. (2025). Development of Intelligent Student Information System. Asian Journal of Basic Science & Research, 7(1): 01–09. http://doi.org/10.38177/ajbsr.2025.7101.

[20] Khan, N.A. (2018). Cloud Applications Development and Deployment: The Future of Cost Effective Programming and a Step Ahead. Middle East Journal of Applied Science & Technology, 1(1): 30–36.

[21] Khan, N.A., et al. (2021). Development of mubadarah system-an intelligent system for proposals at a university. In 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), IEEE. https://doi.org/10.1109/iccike51210.2021.9410773.

[22] Khan, N.A., Rajeyyagari, S., & Khan, A.R. (2025). Development of Intelligent Library Services for University Students. Mediterranean Journal of Basic and Applied Sciences, 9(1): 142–147. https://doi.org/10.46382/mjbas.2025.9109.

[23] Khan, N.A., Siddiqi, A.M.U., & Ahmad, M. (2021). Development of intelligent alumni management system for universities. Asian Journal of Basic Science & Research, 3(2): 51–60. http://doi.org/10.38177/ajbsr.2021.3206.

[24] Akram, F., et al. (2024). Integrating Artificial Bee Colony Algorithms for Deep Learning Model Optimization: A Comprehensive Review. Solving with Bees: Transformative Applications of Artificial Bee Colony Algorithm, Pages 73–102. https://doi.org/10.1007/978-981-97-7344-2_5.

[25] Al Omari, O.M.A., Khan, N.A., & Mahafdah, R. (2017). Ranking and Reputation Based Resource Allocation in P2P System. Mediterranean Journal of Basic and Applied Sciences, 1(1): 293–301.

[26] Alangari, S., & Khan, N.A. (2021). Artificially intelligent warehouse management system. Asian Journal of Basic Science & Research, 3(3): 16–24. http://doi.org/10.38177/ajbsr.2021.3302.

[27] Aljomaee, W.Y., Alshahrani, S.M., & Khan, N.A. (2025). NAMAQ-Arabic Handwriting Recognition Using Deep Learning, AI, and ML with Sentiment Analysis. In 4th International Conference on Computing and Information Technology (ICCIT), IEEE. https://doi.org/10.1109/iccit63348.2025.10989445.

[28] Alshahrani, S.M., et al. (2023). Systematic Survey on Big Data Analytics and Artificial Intelligence for COVID-19 Containment. Computer Systems Science & Engineering, 47(2). https://doi.org/10.32604/csse.2023.039648.

[29] Zamani, A.S., Akhtar, M.M., & Khan, N.A. (2025). An Application of Machine Learning, Big Data and IoT of Enterprise Architecture: Challenges, Solutions and Open Issues. https://doi.org/10.5772/intechopen.1010260.

[30] Khan, N.A., et al. (2024). An IoMT Enabled Iterative Artificial Bee Colony Approach Using Federated Learning for Detection of Heart Disease, in Solving with Bees: Transformative Applications of Artificial Bee Colony Algorithm, Springer, Pages 103–116. https://doi.org/10.1007/978-981-97-7344-2_6.

[31] Khan, N.A., Khan, A.R., & Rajeyyagari, S. (2025). Innovation in teaching and learning with the use of modern computational tools: A Post Covid experience. Middle East Journal of Applied Science & Technology, 8(2): 74–82. https://doi.org/10.46431/mejast.2025.8208.

[32] Khan, N.A., et al. (2020). Internet of Things (IOT) Based Educational Data Mining (EDM) System. J. Mech. Cont. & Math. Sci., 15(3): 271–284. https://doi.org/10.26782/jmcms.2020.03.00022.

[33] Alshahrani, S.M., et al. (2022). URL Phishing Detection Using Particle Swarm Optimization and Data Mining. Computers, Materials & Continua, 73(3). https://doi.org/10.32604/cmc.2022.030982.

[34] Alsulami, M.H., et al. (2021). Zigbee technology to provide elderly people with well-being at home. International Journal of Sensors Wireless Communications and Control, 11(9): 921–927. https://doi.org/10.2174/22103279116 66210201105206.

[35] Hassan, M.A.A., Khan, N.A., & Nasim, M.A. (2017). Managing Data Replication in Mobile Ad-Hoc Network Databases Using Content Based Energy Optimization. Mediterranean Journal of Basic and Applied Sciences, 1(1): 142–154.

[36] Khan, N.A., et al. (2021). An empirical analysis on users' acceptance and usage of BYOD-technology for Saudi universities: a case study of Shaqra University. In 2021 International Conference on Technological Advancements and Innovations (ICTAI), IEEE. https://doi.org/10.1109/ictai53825.2021.9673287.

[37] Khan, N.A., Al-Omari, O.M., & Alshahrani, S.M. (2023). An Empirical Study on the Future of Publication Repositories and Its Adaptability in Public universities—A Case Study of Shaqra University, Saudi Arabia. Computational Intelligence: Select Proceedings of InCITe, Springer, Pages 823–829. https://doi.org/10.1007/978-981-19-7346-8_71.

[38] Khan, N.A., et al. (2024). An IoMT Enabled Iterative Artificial Bee Colony Approach Using Federated Learning for Detection of Heart Disease. In Solving with Bees: Transformative Applications of Artificial Bee Colony Algorithm, Springer, Pages 103–116. https://doi.org/10.1007/978-981-97-7344-2_6.

[39] Khan, N.A. (2025). Statistical probability prediction model for E-Learning and realtime proctoring using IoT devices. Journal of King Saud University – Science, 37: 7002025. https://doi.org/10.25259/jksus_700_2025.