International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

The Impact of Integrating Machine Learning and Block Chain for SMS Spam Detection

Mr. Ravi H Gedam[1], Dr. Sumit Kumar Banchhor[2]
[1]Research Scholar, Department of Computer Science and Engineering Amity School of Engineering and Technology, Amity University Chhattisgarh, Raipur, India.
[2]Assistant Professor, Department of Electronics and Communication Engineering, Amity School of Engineering and Technology, Amity University Chhattisgarh, Village - Manth, Raipur, India.
Email ID: *gedam.hemraj@s.amity.edu[1], skbanchhor@rpr.amity.edu[2]*

Abstract
The widespread use of mobile communication has led to a significant rise in SMS-based spam, posing challenges for users and service providers. This paper explores the integration of machine learning (ML) and block chain technology to enhance SMS spam detection. We assess the effectiveness of various ML algorithms in identifying spam messages and examine the potential of blockchain to provide a secure, decentralized platform for data sharing and model updates. Our findings indicate that combining ML and blockchain can significantly improve the accuracy and reliability of SMS spam detection, offering a comprehensive solution to this growing issue.

Keywords: *SMS Spam Detection, Machine Learning, Block chain Technology, Decentralized Security*

1. Introduction
Spam texts, especially those sent through SMS, have become a real pain in the digital world. These unwanted and unsolicited messages not only annoy the recipients, but also come with serious security risks and can cause significant financial damage. [1] As the volume of SMS traffic continues to rise exponentially, the need for effective and dependable spam detection methods has become increasingly critical. Recent breakthroughs in transformative technologies, such as the smooth fusion of machine learning and blockchain, present highly promising solutions to address the complex and ever-changing challenges associated with SMS spam detection. [2] Tapping into the powerful prediction skills of advanced machine learning, and the built-in safeguards, transparency, and permanence of blockchain tech, gives us a game-changing way to tackle this pesky problem and rein in its far-reaching effects. [3] [4]

2. Background
Spam detection has been a topic of extensive research, with traditional approaches often relying on rule-based filtering or statistical techniques. However, the dynamic and evolving nature of spam tactics has rendered these traditional methods less effective. [5] Machine learning-based approaches have emerged as a more robust and flexible solution, allowing for the development of more advanced spam detection models. [6] These models can leverage linguistic and behavioral patterns, as well as sentence modeling, to identify and classify spam messages with greater accuracy.

2.1. Machine Learning for Spam Detection
Machine learning procedures, such as Long Short-Term Memory and Gated Repetitive Unit, have illustrated promising comes about within the classification of spam emails. [7] These progressed neural arrange models are especially well-suited for taking care of the complexities of printed information, as they can successfully capture the relevant and semantic data implanted inside. [8]

Figure 1 Spam Mail Detection Using Machine Learning

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

LSTM and GRU models use the successive nature of content, permitting them to get it the stream and connections between words, expressions, and sentences. [10] This empowers more nuanced and exact spam discovery, as the models can recognize unobtrusive phonetic designs and behavioral prompts that conventional, rule-based sifting strategies may battle to identify.[11] Besides, the utilize of profound learning calculations, which employ multiple covered up layers to memorize progressively unique representations of the input information, has been appeared to beat conventional, "shallow" machine learning models in an assortment of content classification errands. [5] Besides, the utilize of profound learning calculations, which employ multiple covered up layers to memorize progressively unique representations of the input information, has been appeared to beat conventional, "shallow" machine learning models in an assortment of content classification errands. [12] Figure 1 shows Spam Mail Detection Using Machine Learning

2.2. Block Chain Technology

Blockchain innovation has risen as a promising arrangement for secure and decentralized information administration. Within the setting of SMS spam discovery, blockchain can play a vital part in improving the unwavering quality and straightforwardness of the discovery prepare.[13] By leveraging the unchanging and disseminated nature of blockchain, spam discovery frameworks can make a shared, tamper-resistant record of known spam messages and their related metadata.[14] This data can be gotten to and confirmed by numerous partners, such as arrange suppliers, security offices, and end-users, moving forward the in general reliability and unwavering quality of the spam location framework.[15] Also, blockchain-based smart contracts can be used to computerise the method of spam reporting and blocking then enabling a more effective and responsive framework for dealing with SMS spam.[16]

3. Integrating Machine Learning and Block Chain

By integrating Machine learning (ML) and blockchain techniques presents a groundbreaking approach to real-time threat discovery and avoidance, tending to the developing complexity and advancement of money-related extortion plans. This integration leverages the qualities of both innovations: the predictive control of ML calculations and the transparency, security, and unchanging nature of block chain. [1] Figure 2 Shows Block Chain Machine Learning Integration Flow

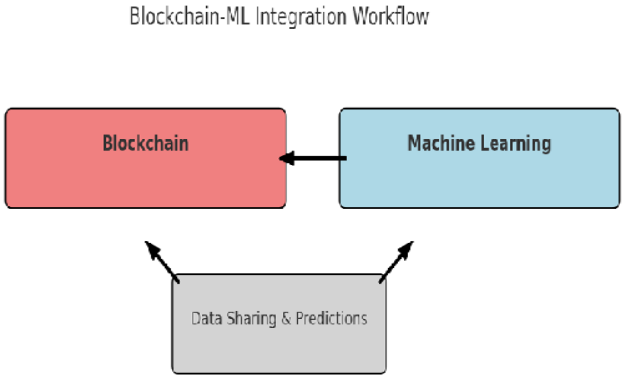

Figure 2 Block Chain Machine Learning Integration Flow

The conceptual framework for joining ML and blockchain incorporates some key components. To start with, data from financial trades is ceaselessly collected and put absent on a blockchain, ensuring straightforwardness and security. ML calculations analyze this data in honest to goodness time, recognizing suspicious plans and hailing potential threats.[18] When a potential danger is recognized, a sharp contract is executed, which can right absent piece the trade, caution the important specialists, or begin advance affirmation forms.[19] This facilitates approach addresses a couple of challenges in ordinary blackmail area systems. The decentralized nature of blockchain murders single centers of disillusionment and reduces the risk of data altering.[20] The straightforwardness of blockchain overhauls the steadfastness of the disclosure handle, while the prescient capabilities of ML provide tall exactness and flexibility to present day blackmail tactics.[21] Also, the real-time dealing with capabilities of both advancements ensure incite revelation and evasion of untrue works.[22]

4. Methodology

The methodology for the study of the impact of

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

integrating machine learning and blockchain for SMS spam detection involves several key steps: Figure 3 shows Methodology of Integrating Machine Learning and Block Chain

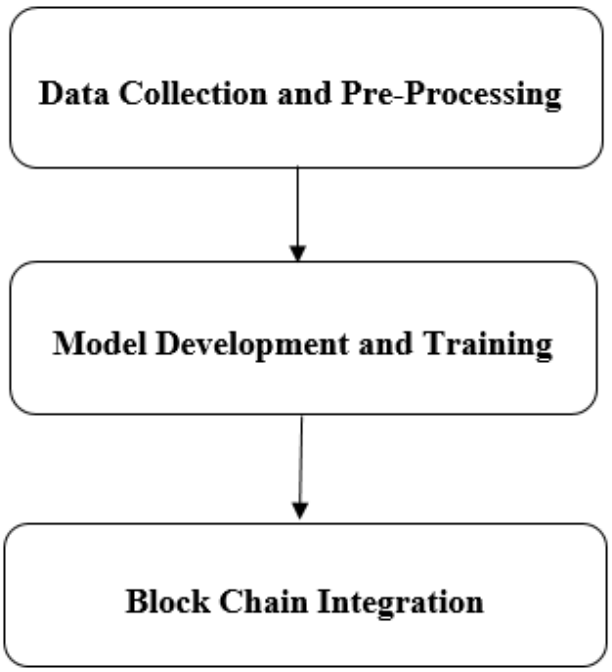

Figure 3 Methodology of Integrating Machine Learning and Block Chain

4.1.Data Collection and Preprocessing

The first step is to collect an extensive dataset of SMS messages, counting both spam and actual messages. Because SMS data is sensitive, open datasets may be compelled to be available. Researchers may have to work with providers or security offices to select access to real-world SMS data while maintaining compliance with assurance guidelines. [23] Once the dataset is obtained, the other step is to preprocess the data, which may incorporate assignments such as substance cleaning, highlight extraction, and the creation of named tests for preparing and testing the machine learning models. [3] The data preprocessing arrangement may be a fundamental step in the enhancement of the facilitated SMS spam disclosure system. The quality, contrasts, and representativeness of the dataset utilized for planning and testing the machine learning models can inside and out influence the common execution and practicality of the framework.[24] Cautious thought must be paid to assignments such as substance cleaning, counting extraction, and the creation of named tests that absolutely reflect the characteristics of real-world SMS messages.[25] Overwhelming preprocessing strategies can offer help to ensure that machine learning models are arranged on high-quality data, driving move-forward accuracy, unflinching quality, and flexibility to develop spam strategies [26] Besides, the preprocessing stage gives an opportunity to address any slants or unbalanced characteristics inside the dataset, which can empower the progress system's capacity to generalize and perform well in real-world scenario.[27]

4.2. Model Development and Training

The centre of the strategy for creating a successful SMS spam location framework is the cautious determination and preparation of machine learning models.[28] Analysts ought to try an assortment of calculations, such as calculated relapse, bolster vector machines, arbitrary timberlands, and profound learning procedures, to decide the foremost appropriate approach for their particular dataset and utilize the case.[29] The preparation handle ought to include thorough strategies to optimize the model's execution. This incorporates utilizing cross-validation to guarantee the model's strength and generalizability, conducting hyperparameter tuning to discover the ideal arrangement of the model's parameters, and leveraging feature engineering to distinguish the foremost instructive characteristics of the SMS data. [30] [31] Through these key steps, analysts can create a profoundly precise and dependable machine learning-based spam location framework custom fitted to their needs.

4.3. Block Chain Integration

The following step within the technique is to coordinate the machine learning-based SMS spam discovery framework with a blockchain-based design. This includes planning and actualizing a disseminated, decentralized framework that leverages the capabilities of blockchain innovation to upgrade the security, straightforwardness, and collaboration perspectives of the spam discovery process. [32] Key components of the blockchain integration incorporate:

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

- **Smart Contract Design:** Creating keen contracts that typify the rules and rationale for the SMS spam discovery handle, counting the accommodation of SMS messages, the classification of messages as spam or authentic, and the recording of spam-related data on the block chain. [33]
- **Distributed Storage:** Utilizing the blockchain's decentralized capacity capabilities to safely store the SMS message information, as well as the prepared machine learning models and any related metadata.[34]
- **Consensus Mechanism:** Implementing a suitable consensus mechanism, such as Proof-of-Work or Proof-of-Stake, to ensure the integrity and immutability of the spam detection records on the blockchain.[35]
- **Decentralized Collaboration:** Enabling a decentralized network of participants, such as network providers, security agencies, and researchers, to contribute to the spam detection process and share information, while maintaining the privacy and confidentiality of the data.[24]
- **Integration with Existing SMS Platforms:** Developing the necessary interfaces and protocols to seamlessly integrate the blockchain-based SMS spam detection system with existing SMS communication platforms, ensuring a smooth and transparent user experience. [36]

5. Impact of the integration

5.1.Advantages of the Integration

The integration of machine learning and blockchain for SMS spam location offers several advantages:

- Improved Precision: The combination of advanced machine learning calculations and the organized, tamper-resistant data capacity of blockchain can lead to more exact and reliable spam locations, reducing the number of false positives and false negatives.[37]
- Upgraded Transparency and Responsibility: The blockchain-based ledger of known spam messages and their metadata gives a straightforward and verifiable framework, permitting way better oversight and responsibility within the spam location process. [38], [39]
- Computerized and Responsive Moderation: The use of blockchain-based keen contracts can empower robotized and quick reaction components to moderate the effect of SMS spam, reducing the burden on manual mediation and moving forward the in general productivity of the system. [40]
- Diminished Costs: By streamlining the spam location and relief forms, the integration of machine learning and blockchain can lead to fetched reserve funds for organized suppliers and end-users, as the requirement for manual survey and intercession is reduced. [22]
- Versatility to Advancing Dangers: The machine learning component of the framework can persistently learn and adjust to unused spam strategies, guaranteeing the location capabilities stay compelling against developing threat. [41]
- Decentralized and Secure Framework: The blockchain-based design gives a decentralized and secure framework, lessening the hazard of single focuses of disappointment and information altering, which are common vulnerabilities in centralized spam discovery systems. [42]
- Progressed Client Encounter: By viably identifying and relieving SMS spam, the coordinates framework can upgrade the by and large client involvement, lessening the effect of undesirable messages and making strides within the communication channels.[43]
- Collaborative Spam Detailing and Relief: The shared nature of the blockchain-based framework can cultivate collaboration among organized suppliers, security offices, and end-users, empowering a more comprehensive and viable approach to distinguishing, detailing, and moderating SMS spam.[44]

5.2.Challenges and Limitations

However, the fruitful usage of these methods within the setting of SMS spam location remains a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

challenge, as the constrained length and one of a kind characteristics of brief content messages can pose troubles for conventional sifting arrangements.

Moreover, the integration of machine learning and blockchain innovations presents its claim set of challenges, counting:

- Information Protection and Administrative Compliance: Guaranteeing the assurance of client security and compliance with information assurance controls, such as GDPR, can be a critical challenge when managing with the capacity and handling of touchy individual data on a blockchain. [45]
- Adaptability and Execution: Accomplishing high-throughput preparation and real-time decision-making for SMS spam location whereas keeping up the adaptability and execution of the coordinates framework can be a specialized hurdle. [46]
- High fee: As exchange volumes increment, blockchain stages may involve delays in exchange affirmations and higher handling fees. [47]
- Computational Overhead: The combination of machine learning calculations and blockchain operations may present additional computational overhead, which has to be carefully overseen to guarantee the proficiency and cost-effectiveness of the system. [48]
- Interoperability and Integration: Coordination of the SMS spam discovery framework with existing communication stages and framework can be complex, requiring cautious thought of compatibility and consistent integration. [49]

Conclusion

In conclusion, the integration of machine learning and blockchain advances presents a promising approach to tending to the developing challenge of SMS spam.[50] By combining the capable design acknowledgment capabilities of machine learning with the secure, straightforward, and decentralized nature of blockchain, this coordinates framework can give a more compelling and vigorous arrangement for SMS spam location and mitigation.[41] Whereas there are still challenges and impediments to be tended to, the potential benefits of this integration, such as progressed exactness, upgraded straightforwardness, robotized moderation, and decreased costs, make it a compelling zone for assisting investigation and improvement.[51]

Future Research Direction

Based on the discoveries of this ponder, a few roads for future investigations can be investigated:

- Investigating more advanced machine learning techniques, such as deep learning and reinforcement learning, to improve the accuracy and adaptability of SMS spam detection. [52]
- Investigating the utilize of unified learning or other privacy-preserving machine learning approaches to address information security concerns in a blockchain-based system. [53]
- Developing an effective calculations and information structures to optimize the computational execution and versatility of the coordinates system. [54]
- Analyzing the financial suggestions and taking a toll model of the blockchain-based SMS spam discovery framework, counting the effect of exchange expenses and the potential for motivating force mechanisms. [55]
- Examining the interoperability and integration challenges of the framework with existing communication stages and framework, and proposing arrangements to upgrade the consistent sending and selection of the technology. [56]

References

[1]. H. O. Bello, C. Idemudia, and T. V. Iyelolu, “Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention,” Jul. 07, 2024, GSC Online Press. doi: 10.30574/wjarr.2024.23.1.1985.

[2]. S. Hosseinpour and H. Shakibian, “Complex-Network based model for SMS spam filtering,” Nov. 09, 2024, Elsevier BV. doi: 10.1016/j.comnet.2024.110892.

[3]. V. S. Vinitha, D. K. Renuka, and L. A.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

Kumar, "Long Short-Term Memory Networks for Email Spam Classification," Feb. 09, 2023. doi: 10.1109/iciscois56541.2023.10100445.

[4]. Y. Maleh, M. Alazab, L. Tawalbeh, and I. Romdhani, "Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence," Mar. 15, 2023. doi: 10.1201/9781003373384.

[5]. A. Sheneamer, "Comparison of Deep and Traditional Learning Methods for Email Spam Filtering," Jan. 01, 2021, Science and Information Organization. doi: 10.14569/ijacsa.2021.0120164.

[6]. H. Al-Kaabi, A. D. Darroudi, and A. N. Jasim, "Survey of SMS Spam Detection Techniques: A Taxonomy," Dec. 25, 2024. doi: 10.61710/kjcs.v2i4.88.

[7]. I. Basyar, A. Adiwijaya, and D. T. Murdiansyah, "Email Spam Classification Using Gated Recurrent Unit and Long Short-Term Memory," Apr. 01, 2020, Science Publications. doi: 10.3844/jcssp.2020.559.567.

[8]. T. Muralidharan and N. Nissim, "Improving malicious email detection through novel designated deep-learning architectures utilizing entire email," Sep. 17, 2022, Elsevier BV. doi: 10.1016/j.neunet.2022.09.002.

[9]. A. Qazi, N. Hasan, R. Mao, M. E. Abo, S. K. Dey, and G. Hardaker, "Machine Learning-Based Opinion Spam Detection: A Systematic Literature Review," Jan. 01, 2024, Institute of Electrical and Electronics Engineers. doi: 10.1109/access.2024.3399264.

[10]. A. Miranda-García et al., "Deep learning applications on cybersecurity: A practical approach," Oct. 07, 2023, Elsevier BV. doi: 10.1016/j.neucom.2023.126904.

[11]. M. K. Khan, A. Buriro, T. Ahmad, and S. Ullah, "Backdoor Malware Detection in Industrial IoT Using Machine Learning," Jan. 01, 2024. doi: 10.32604/cmc.2024.057648.

[12]. M. R. A. Saidat, S. Y. Yerima, and K. Shaalan, "Advancements of SMS Spam Detection: A Comprehensive Survey of NLP and ML Techniques," Jan. 01, 2024, Elsevier BV. doi: 10.1016/j.procs.2024.10.198.

[13]. T. Ashfaq et al., "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism," Sep. 21, 2022, Multidisciplinary Digital Publishing Institute. doi: 10.3390/s22197162.

[14]. J. Seol and J. Kim, "Machine Learning Ensures Quantum-Safe Blockchain Availability," Jan. 31, 2024, Taylor & Francis. doi: 10.1080/08874417.2024.2308207.

[15]. O. Akanfe, D. Lawong, and H. R. Rao, "Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities," Jan. 16, 2024, Elsevier BV. doi: 10.1016/ j.ijinfomgt. 2024.102753.

[16]. S. A. Joseph, "Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems," Sep. 07, 2024. doi: 10.9734/jerr/2024/v26i91271.

[17]. M. S. A. AFNAN, C. Yzem, F. Yuan, and J. Wang, "A Comprehensive Review of the Integration of Machine Learning into Blockchain Technology," Nov. 06, 2024. doi: 10.20944/preprints202411.0146.v1.

[18]. P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter SMS Spam," Sep. 04, 2019, Elsevier BV. doi: 10.1016/j.future.2019.09.001.

[19]. M. Faheem and M. A. Al-Khasawneh, "Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks," May 03, 2024, Elsevier BV. doi: 10.1016/j.dib.2024.110461.

[20]. G. Waja, G. Patil, C. Mehta, and S. Patil, "How AI Can be Used for Governance of Messaging Services: A Study on Spam Classification Leveraging Multi-Channel Convolutional Neural Network," Dec. 22,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

2022, Elsevier BV. doi: 10.1016/j.jjimei.2022.100147.

[21]. J. Ahmad et al., "Machine learning and blockchain technologies for cybersecurity in connected vehicles," Sep. 19, 2023, Wiley. doi: 10.1002/widm.1515.

[22]. A. Valencia-Arías, J. D. González-Ruíz, L. V. Flores, L. Vega-Mori, P. A. Rodríguez-Correa, and G. S. Santos, "Machine Learning and Blockchain: A Bibliometric Study on Security and Privacy," Jan. 22, 2024, Multidisciplinary Digital Publishing Institute. doi: 10.3390/info15010065.

[23]. H. C. Altunay and Z. Albayrak, "SMS Spam Detection System Based on Deep Learning Architectures for Turkish and English Messages," Dec. 17, 2024, Multidisciplinary Digital Publishing Institute. doi: 10.3390/app142411804.

[24]. A. Hajian, R. Sadeghi, V. R. Prybutok, and C. E. Koh, "Increasing trust and value of mobile advertising in retailing: A survey design, machine learning approach, and blockchain in the trust path," Mar. 12, 2024, Elsevier BV. doi: 10.1016/j.jretconser.2024.103794.

[25]. M. Alshurideh, S. Hamadneh, H. M. Alzoubi, B. A. Kurdi, M. T. Nuseir, and A. A. Hamad, "Empowering Supply Chain Management System with Machine Learning and Blockchain Technology," Jan. 01, 2024, Springer International Publishing. doi: 10.1007/978-3-031-31801-6_21.

[26]. Z. A. Siddiqui and M. Haroon, "Application of artificial intelligence and machine learning in blockchain technology," Jan. 01, 2022, Elsevier BV. doi: 10.1016/b978-0-12-824054-0.00001-0.

[27]. P. V. P. Raj and A. M. Khedr, "SDCBM: A Secure Data Collection Model with Blockchain and Machine Learning Integration for Wireless Sensor Networks," Jan. 01, 2025, IEEE Sensors Council. doi: 10.1109/jsen.2025.3526807.

[28]. I. Sood and V. Sharma, "TLERAD: Transfer Learning for Enhanced Ransomware Attack Detection," Jan. 01, 2024. doi: 10.32604/cmc.2024.055463.

[29]. F. Nawshin, R. Gad, D. Ünal, A. Al-Ali, and P. N. Suganthan, "Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey," Apr. 11, 2024, Elsevier BV. doi: 10.1016/j.compeleceng.2024.109233.

[30]. R. H. Chowdhury, "The evolution of business operations: unleashing the potential of Artificial Intelligence, Machine Learning, and Blockchain.," Jun. 30, 2024, GSC Online Press. doi: 10.30574/wjarr.2024.22.3.1992.

[31]. N. Al-shanableh, M. Alzyoud, and E. Nashnush, "Enhancing Email Spam Detection Through Ensemble Machine Learning: A Comprehensive Evaluation Of Model Integration And Performance," Sep. 20, 2024. doi: 10.58729/1941-6687.1451.

[32]. Y. Xu, G. Xu, Y. Liu, Y. Liu, and M. Shen, "A survey of the fusion of traditional data security technology and blockchain," May 06, 2024, Elsevier BV. doi: 10.1016/j.eswa.2024.124151.

[33]. Ş. Kayıkçı and T. M. Khoshgoftaar, "Blockchain meets machine learning: a survey," Jan. 06, 2024, Springer Science+Business Media. doi: 10.1186/s40537-023-00852-y.

[34]. E. Fazel, M. Z. Nezhad, J. Rezazadeh, M. Moradi, and J. Ayoade, "IoT convergence with machine learning & blockchain: A review," Apr. 21, 2024, Elsevier BV. doi: 10.1016/j.iot.2024.101187.

[35]. A. M. S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," Feb. 29, 2024, Elsevier BV. doi: 10.1016/j.bcra.2024.100193.

[36]. V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, "Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity," Jan. 21, 2022, Elsevier BV. doi:

10.1016/j.ijinfomgt.2022.102470.
[37]. S. Dhar and I. Bose, "An ensemble deep learning model for fast classification of Twitter spam," Oct. 01, 2024, Elsevier BV. doi: 10.1016/j.im.2024.104052.
[38]. T. Amutha and S. Geetha, "Automated Spam Detection Using Sandpiper Optimization Algorithm-Based Feature Selection with the Machine Learning Model," Nov. 23, 2023, Taylor & Francis. doi: 10.1080/03772063.2023.2280663.
[39]. S. Kumar, Shersingh, S. kumar, and K. verma, "Malware Classification Using Machine Learning Models," Jan. 01, 2024, Elsevier BV. doi: 10.1016/ j.procs. 2024.04.133.
[40]. Z. T. Pritee, M. H. Anik, S. B. Alam, J. R. Jim, Md. M. Kabir, and M. F. Mridha, "Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review," Feb. 12, 2024, Elsevier BV. doi: 10.1016/j.cose.2024.103747.
[41]. N. Innab et al., "Phishing Attacks Detection Using Ensemble Machine Learning Algorithms," Jan. 01, 2024. doi: 10.32604/cmc.2024.051778.
[42]. X. Yi, S. Lin, X. Jia, and S. Gao, "Design and implementation of commercial SMS supervision model based on blockchain," Dec. 16, 2022. doi: 10.1117/12.2660804.
[43]. Z. Dong and W. Lu, "Machine Learning on Blockchain (MLOB): A New Paradigm for Computational Security in Engineering," Dec. 01, 2024, Elsevier BV. doi: 10.1016/j.eng.2024.11.026.
[44]. I. Dimitriadis, G. Dialektakis, and A. Vakali, "CALEB: A Conditional Adversarial Learning Framework to enhance bot detection," Nov. 14, 2023, Elsevier BV. doi: 10.1016/j.datak.2023.102245.
[45]. T. Sivaram and B. Saravanan, "Recent Developments And Challenges Using Blockchain Techniques For Peer-To-Peer Energy Trading: A Review," Dec. 01, 2024, Elsevier BV. doi: 10.1016/ j.rineng.2024.103666.
[46]. S. B. Far and M. R. Asaar, "A blockchain-based anonymous reporting system with no central authority: Architecture and protocol," Dec. 12, 2023, Elsevier BV. doi: 10.1016/j.csa.2023.100032.
Z. Ruan, "Blockchain Technology for Security Issues and Challenges in IOT," Nov. 15, 2023. doi: 10.1109/csmis60634.2023.00108.
[47]. O. O. Khalifa, T. H. S. B. T. N. Effendy, M. Z. Ahmed, E. A. Elkhazmi, and A. N. Esgiar, "Blockchain Based Email Security to Mitigate Phishing Attack," Dec. 20, 2024. doi: 10.69955/ajoeee.2024.v4i2.73.
[48]. A. Nazir et al., "Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration," Feb. 01, 2024, Elsevier BV. doi: 10.1016/j.jksuci.2024.101939.
[49]. S. Sh. Taher, S. Y. Ameen, and J. A. Ahmed, "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach," Feb. 08, 2024, Engineering, Technology & Applied Science Research. doi: 10.48084/etasr.6641.
[50]. R. O. Ogundokun, M. O. Arowolo, R. Damaševičius, and S. Misra, "Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning," May 31, 2023, Multidisciplinary Digital Publishing Institute. doi: 10.3390/ telecom4020017.
[51]. R. Salama, C. Altrjman, and F. Al-Turjman, "An overview of future cyber security applications using AI and blockchain technology," Jan. 01, 2024, Elsevier BV. doi: 10.1016/b978-0-443-13268-1.00020-0.
[52]. H. Lakhdar, F. Elmendili, and Y. E. B. E. Idrissi, "Blockchain-based spam detection approach," Oct. 26, 2023. doi: 10.1109/wincom59760.2023.10323001.
[53]. J. Ali et al., "A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks," Nov. 12, 2024, Elsevier BV. doi:

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 592 - 600
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0083

10.1016/j.comcom.2024.108000.

[54]. G. Nasreen, M. M. Khan, M. Younus, B. Zafar, and M. K. Hanif, "Email spam detection by deep learning models using novel feature selection technique and BERT," Apr. 30, 2024, Elsevier BV. doi: 10.1016/j.eij.2024.100473.

[55]. A. Qazi, N. Hasan, R. Mao, M. E. Abo, S. K. Dey, and G. Hardaker, "Machine Learning-Based Opinion Spam Detection: A Systematic Literature Review," Jan. 01, 2024, Institute of Electrical and Electronics Engineers. doi: 10.1109/ access.2024. 3399264.