International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Enhanced SMS Spam Detection Framework Using Blockchain and Machine Learning

Mr. Ravi H. Gedam, Dr. Sumit Kumar Banchhor

Submitted: 02/05/2024 **Revised**: 15/06/2024 **Accepted**: 22/06/2024

Abstract: - SMS spam has become a persistent, causing issues for mobile consumers throughout the world. Traditional spam detection technologies frequently fail to adequately identify and filter undesirable communications. In answer to this difficulty, this study proposes a novel architecture that combines blockchain technology and machine learning approaches to improve SMS spam detection. The framework uses blockchain's decentralised and irreversible characteristics to create a transparent and safe platform for gathering labelled SMS data from consumers. This data is then used to train machine learning models, which use a variety of strategies to increase classification accuracy, including natural language processing and ensemble methods. The efficacy and efficiency of the proposed system in identifying SMS spam while protecting user privacy are proved experimentally. The report also analyses the possible consequences of using blockchain in spam detection systems and proposes future research goals in this area. Overall, this approach marks a big step forward in combatting SMS spam and helps to continuing efforts to improve cybersecurity and consumer privacy in the mobile communication ecosystem.

Keywords: - *SMS Spam Detection, Blockchain, Machine Learning, Detection Spam Filtering*

1. Introduction

Short Message Service (SMS) has become an indispensable part of modern communication, providing a ubiquitous means of exchanging information and staying connected. However, in addition to their widespread use, SMS platforms have become a target for unscrupulous actors attempting to broadcast undesired and often dangerous material, known as SMS spam [1]. SMS spam proliferation poses significant challenges for both mobile users and service providers, ranging from inconvenience and annoyance to major security risks and financial fraud.

Traditional SMS spam detection systems rely heavily on rule-based filtering and heuristics, which regularly fall behind new spamming strategies and trends. Furthermore, centralised spam detection systems have inherent vulnerabilities, such as single points of failure, data manipulation, and privacy concerns. In this environment, there is an urgent need for breakthrough solutions that may increase the efficiency, reliability, and security of SMS spam detection.

To solve these issues, this study suggests an enhanced SMS spam detection system that takes advantage of the synergies between blockchain technology and machine learning algorithms. Blockchain, being a decentralised and irreversible ledger, has distinct benefits for assuring data integrity, transparency, and trust in SMS spam detection systems. Blockchain, by decentralising SMS data storage and processing, can reduce the dangers associated with centralised infrastructures, such as data tampering and unauthorised access[2]. Furthermore, machine learning approaches offer effective tools for analysing and categorising SMS messages based on their content and context. Machine learning algorithms may learn to discriminate between two categories with high accuracy and flexibility by training prediction models on labelled datasets of authentic and spam communications. Integrating machine learning with blockchain allows for the development of a dynamic and resilient spam detection system [3] that can continually improve its effectiveness over time.

1Research Scholar, Department of COMPUTER SCIENCE AND ENGINEERING Amity School of Engineering and Technology, Amity University Chhattisgarh, Raipur
Gedam.hemraj@s.amity.edu
2Assistant Professor Department of Electronics and Communication Engineering Amity School of Engineering and Technology Amity University Chhattisgarh, Village – Manth, Raipur
skbanchhor@rpr.amity.edu

1.1 Background

The proliferation of spam messages via SMS (Short Message Service) is a major worry for both users and telecoms operators. Traditional spam detection systems, which depend on static rule sets or heuristics, can occasionally fall behind shifting spamming methods. To address this challenge, researchers and practitioners have investigated merging machine learning (ML) techniques to increase spam detection flexibility and accuracy. Conventional ML models, on the other hand, face challenges in assuring the integrity and transparency of their decision-making processes since they usually operate in centralised systems that allow for data manipulation or tampering [4]. In response, blockchain technology has emerged as a feasible tool for increasing the security and reliability of spam detection algorithms. Researchers want to create a decentralised, immutable, and transparent SMS spam detection system by combining machine learning algorithms with blockchain. Blockchain secures data integrity and prevents unauthorised alterations, whilst machine learning algorithms analyse incoming SMS texts to accurately detect spam tendencies. This integrated solution increases spam detection reliability and accuracy while simultaneously addressing data privacy and security concerns. Overall, the combination of blockchain and machine learning offers significant potential for combating SMS spam by offering a robust and transparent framework capable of adapting to evolving spamming methods while ensuring the integrity and security of user data [5].

1.2 Objectives

The goals of an improved SMS spam detection system using blockchain and machine learning are varied. To begin, the framework intends to dramatically increase the accuracy and efficiency of spam identification in SMS conversations, hence improving user experience and mitigating the harmful impact of spam messages. Using machine learning algorithms, the system aims to continually learn and adapt to new spamming strategies, assuring proactive identification of developing spam trends. Second, the use of blockchain technology assures data integrity, transparency, and immutability, reducing the dangers of data tampering or manipulation [6]. This increases the credibility of the spam detection process and builds trust among users and stakeholders. Furthermore, the framework aims to solve data privacy and security issues by implementing a decentralised architecture that secures user information from unauthorised access or abuse. By attaining these goals, the upgraded SMS spam detection framework hopes to provide a strong, dependable, and transparent system that efficiently combats spam while protecting user privacy and confidence.

1.3 SMS Spam Detection

SMS spam detection is the act of recognising and filtering unwanted and possibly hazardous communications transmitted by Short Message Service (SMS). With the growing use of mobile phones and text messaging, SMS spam has grown in importance, causing consumers trouble, frustration, and, in some cases, financial loss. Traditional SMS spam detection technologies [7] frequently rely on rule-based filters and heuristics, which may struggle to keep up with developing spamming strategies. Advanced techniques use machine learning algorithms to analyse message content and context in order to detect messages more accurately. In addition, some systems use blockchain technology to improve security, transparency, and confidence in the spam detection process by decentralising data storage and maintaining data integrity. SMS spam detection [8] strives to equip consumers and service providers with powerful tools for combating unwanted messages and ensuring a safe messaging environment.

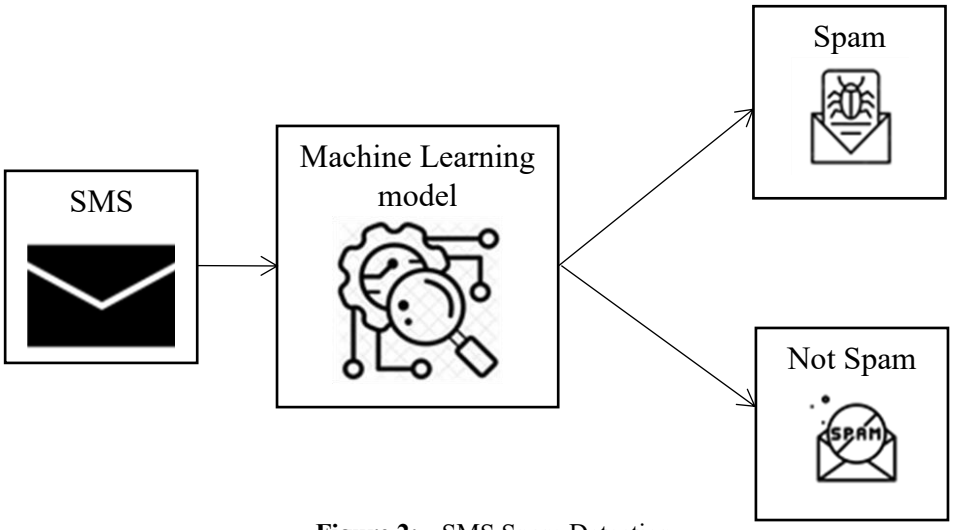


Figure 2: - SMS Spam Detection

1.4 Detection Framework

A detection framework is an organised strategy or system for identifying and analysing certain occurrences or events within a given environment. Detection frameworks in sectors such as cybersecurity, fraud detection, and healthcare often include a collection of tools, procedures, and algorithms designed to recognise trends, abnormalities, or risks. These frameworks frequently use machine learning, data analysis, and statistical modelling [9] approaches to improve the accuracy and efficiency of finding pertinent information. The ultimate purpose of a detection framework is to give timely and reliable insights or warnings that aid decision-making and minimise risks or vulnerabilities inside the system or environment in which it functions.

1.5 Framework Using Blockchain

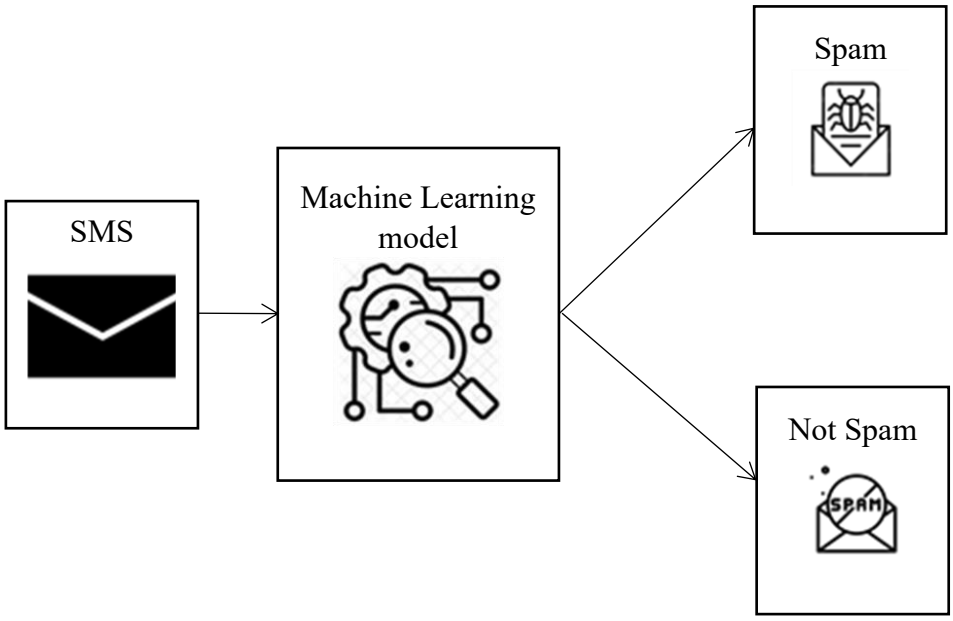
A blockchain framework is often defined as a structured strategy or system that includes blockchain technology as a core component. Blockchain is a decentralised, distributed ledger system that securely and permanently records transactions over a network of computers. Blockchain frameworks [10] are used in a variety of fields, including banking, supply chain management, and healthcare, to improve transparency, security, and trust by providing a tamper-proof and transparent record of data exchanges. These frameworks frequently include smart contracts, cryptographic algorithms, and consensus procedures to maintain data integrity and enable trustless interactions among participants. Blockchain integration into frameworks has the potential to allow novel solutions for a wide range of use cases, including digital identity management, supply chain traceability, and decentralised finance.

1.6 Types Of SMS Spam Detection

- **Keyword-based Filtering**: This method identifies spam communications by analysing particular terms or phrases that are frequently linked with spam. Messages that include these keywords are marked as spam.
- **Rule-based Filtering**: Rule-based filtering, like keyword-based filtering, requires developing rules or patterns to identify spam communications based on criteria such as sender information, message content, and layout.
- **Machine Learning Algorithms**: Machine learning algorithms may be trained to categorise communications as spam or non-spam based on a range of characteristics, including message content, sender behaviour, and metadata. Naive Bayes, Support Vector Machines (SVM), and Random Forests are among the most often used algorithms.
- **Behavioral Analysis**: This method entails analysing user behaviour and interaction patterns to find abnormalities indicating spam activity. Spam can be identified by rapid surges in message volume or strange sending patterns, for example.
- **Collaborative Filtering**: Collaborative filtering approaches employ collective intelligence to detect spam communications by analysing comments from different users. Users report spam messages, and the system uses this data to enhance spam detection accuracy across the whole user base.

1.7 Importance Of Spam Detection Framework Using Blockchain

The relevance of a blockchain-based spam detection system stems from its potential to provide a safe, transparent, and decentralised way to prevent the spread of unwelcome communications. Blockchain technology guarantees that spam detection operations are recorded in a tamper-proof and irreversible way, which increases confidence and transparency in the detection process. This decentralised method lowers the danger of spam detection data modification or corruption, improving the framework's dependability and integrity. Furthermore, blockchain provides more efficient collaboration and information exchange among network users, allowing for the quick detection and mitigation of spam across several communication channels. Using blockchain technology into spam detection frameworks improves the efficacy, security, and reliability of combatting unwelcome communications in digital communication networks.



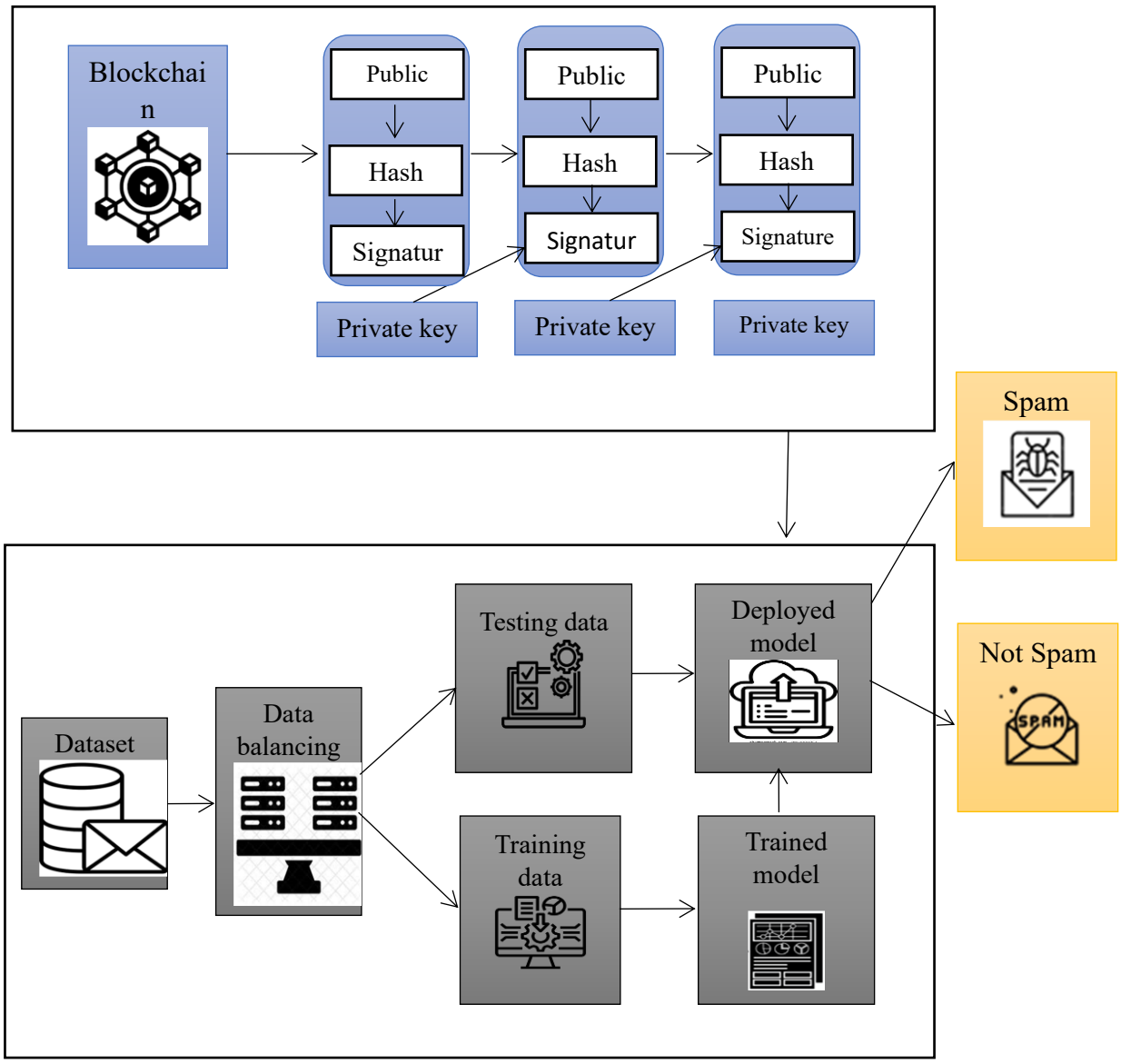


Figure 1: The suggested blockchain and machine learning system architecture.

Figure 1 displays the prediction result indicating whether a blockchain-based transaction is malicious or lawful after it has been confirmed using a machine learning model. A dataset including bitcoin transaction data serves as the basis for training and validating the machine learning model's prediction.

1.8 Motivation

The value of a blockchain-based spam detection system stems from its capacity to provide a safe, transparent, and decentralised approach to prevent the spread of unwelcome communications. Blockchain technology guarantees that spam detection operations are stored in a tamper-resistant and immutable format, increasing confidence and transparency in the detection process. This decentralised method decreases the possibility of spam detection data being manipulated or corrupted, improving the framework's dependability and integrity. Furthermore, blockchain allows for more effective collaboration and information exchange among network users, helping the speedy detection and mitigation of spam across numerous communication channels. Overall, using blockchain technology into spam detection frameworks improves the efficacy, security, and reliability of countering unwelcome communications in digital communication networks.

2. Literature Review

The provided text outlines a wide array of research studies and advancements in the realm of cybersecurity, focusing on diverse topics such as spam detection, IoT security, malware detection, and online moderation. Researchers are leveraging machine learning (ML) and deep learning (DL) techniques to enhance the accuracy of spam detection in emails and SMS, with studies showcasing the effectiveness of support vector machines (SVM) and LightGBM algorithms in identifying spam messages. Additionally, the integration of blockchain technology with ML models is explored to bolster security in IoT sensor networks, while innovative approaches like hybrid deep learning architectures are proposed for detecting SMS spam with remarkable accuracy. Moreover, there are efforts to combat malware through explainable machine learning methods and improve online moderation using large language models (LLMs). Ethical hacking simulations emerge as a strategy for identifying and mitigating security flaws in IoT devices, emphasizing the importance of proactive security measures in the face of evolving cyber threats. These studies collectively contribute to advancing cybersecurity practices and addressing the challenges posed by malicious activities in digital environments.

Malicious assaults like spam and phishing emails are on the rise due to the exponential growth in the use of SMS and email. The accuracy of current machine learning (ML) models in identifying these risks has not reached 100%. To improve spam detection accuracy, Umair Maqsood et al. [11] looked into a variety of machine learning (ML) and deep learning (DL) classifiers. Email and SMS datasets were subjected to many classifier applications. SVM, or support vector machine, turned out to be the best. The research showed that SVM performed better than other classifiers in terms of reliably identifying spam in datasets of emails and SMS. This implies that SVM is better at classification jobs like spam identification. The security of Internet of Things (IoT) sensor networks is greatly challenged by cyberattacks, which calls for the creation of effective countermeasures that are specific to their needs and constraints. To safeguard IoT sensor networks, Shereen Ismail et al. [12] investigated an integrated security framework that combines machine learning (ML) and blockchain technology. The two modules that make up the framework are the ML detection module and the BC prevention module. The research illustrated how well the integrated security framework works to prevent cyberattacks on Internet of Things sensor networks. After a thorough comparison examination of assessment measures, LightGBM was determined to be the best option among the several ML algorithms that were studied. Worldwide, SMS spam is a major problem that can lead to inconvenience, waste of time, and even financial scams. To lessen the impact of SMS spam, accurate and timely detection is essential. Five stages make up Hussein Alaa Al-Kabbi's et al. [13] innovative method for detecting SMS spam: preprocessing, feature extraction, feature fusion, feature selection, and classification. To improve feature representation, the model concurrently captures local, temporal, and global text message properties through the use of a hybrid deep learning architecture. With a high accuracy of 99.56%, the suggested method outperformed both conventional and deep learning methods, including RF and BERT. This research indicates that the approach has the potential to be used in the real world by showing how well it reduces the incidence and effects of SMS spam. Examined the frequency of phishing assaults and their effects with the goal of locating current defensive techniques, typical phishing vectors, and recommendations for end users and businesses. Bilal Naqvi et al. [14] After a comprehensive review of the literature, 248 papers from reputable digital libraries that covered the time frame from March 2023 to early 2018 were looked at. The research primary objectives were to identify current mitigation techniques, underlying technology, typical phishing vectors, and anti-phishing best practices. The research found many ways to counteract phishing attempts and emphasized the significance of taking into account the capabilities of human users in addition to technology-focused solutions. Accompanying the identification of holes and unresolved problems in the current state of the art surrounding phishing assaults were recommendations for companies and end users. The predictive power of Twitter analytics in the medical domain was examined in the face of the dissemination of incorrect information, with the aim of distinguishing reality from fiction by Carlos Cano-Marin et al. [15]and associate. A thorough review of the literature was conducted in order to analyze Twitter applications for healthcare prediction in addition to recent scholarly studies. Public health issues and mental health illnesses were

two crucial prediction applications that the study identified. It was important to investigate the veracity of health-related content posted on Twitter, paying particular attention to Covid-19. It is critical to ensure strong security in the context of the Internet of Things (IoT).

By fusing blockchain technology with machine learning (ML) models, Ahsan Nazir's et al. [16] research offers a revolutionary way to improve IoT security. In the framework of a collaborative threat intelligence framework for IoT security, the research applies CNN, LSTM, Random Forest, Ensemble, and Decision Tree classifier models on the IoT23 dataset. By decreasing false negatives using the collaborative threat intelligence system, the models' accuracy is enhanced iteratively. The efficacy of the suggested approach in augmenting IoT security is exhibited by means of experimental assessments conducted on the IoT23 dataset. Seaports now face new difficulties from Industry 4.0 and the COVID-19 pandemic, which calls for an overhaul of their information systems to make them more competitive in the global market. In order to integrate transactional data among logistics players, Claudia Durán et al. [17] conducted research on the Dependable Machine Learning for Seaports using Blockchain (DMLBC) approach. For safe and effective port operations, DMLBC uses machine learning and blockchain technologies. The effectiveness of DMLBC for decision-making in port operations was demonstrated through a genuine case research implementation. The research compares the benefits of DMLBC to other methods and explores potential avenues for further research to improve maritime efficiency and security. The continuous nature of SMS spam makes it a significant danger to public safety. Thus, it is necessary to investigate systems that can withstand the deceptive strategies employed by spammers. In his exploration on the difficulties associated with SMS spam detection and filtering, Muhammad Salman et al. [18] provided a fresh dataset of more than 68K SMS messages for research. Semantic and syntactic elements were taken out in order to assess and contrast different machine learning-based SMS spam detection techniques. The research found that popular anti-spam services and shallow machine learning algorithms performed poorly in reliably categorizing SMS spam messages. Research is required to improve SMS spam detection and anti-spam services, as current methods are vulnerable to several evasion techniques used by spammers. Due to the malware's quick spread, realistic methods of detecting it are required. In-depth feature building is necessary for current machine learning-based methods, which limits their usefulness. Explainable machine learning techniques were used by Ahsan Wajahat et al. [19] to research a lightweight Android malware detection solution. Malicious and benign apps are distinguished by the system using features that are taken from mobile apps. Excellent accuracy and an F1-score more than 0.99 were found in the investigation. With minuscule false positive and false negative rates, the system uses very little device resources. Transparency and interpretability of the classifier model are improved by Shapley's additive explanation scores. Large language models (LLMs) are being used to moderate online discussions; the focus is on comprehending user intent and problematic material. Toxic language and debate derailment are identified in talks using content classification techniques such as sentiment analysis and keyword extraction. LLMs are used to develop moderation tool prototypes that are tested on German and English datasets by Christoph Gehweiler et al. [20]. The usefulness of the created instruments is assessed, providing information about content categorization and the shortcomings of the existing LLMs, especially with regard to false positives. They explore ways to improve model fine-tuning to support online moderation initiatives.

The identification of unsolicited spam emails is hampered by low detection rates and a high probability of false alarms. Femi Emmanuel Ayo et al. [21] has presented a hybrid correlation-based deep learning model for classifying spam emails. To overcome these difficulties, this model makes use of a rule-based hybrid feature selection method as well as a fuzzy inference system. Comparing the created method to existing machine learning techniques, the F1-score results are better, with 96.5% for the test set spambase and 96.4% for the test set non-spam base. Furthermore, it displays improved processing speed, accuracy, and error rate of 0.5 s, 5.9983%, and 94.0017%, respectively. Additionally, the suggested method lowers misclassification using the fuzzy inference system. Machine learning research has seen a significant shift due to the impressive performance of Deep Learning (DL), especially with Large Language Models (LLMs), which have been demonstrated in a variety of areas. Wahab Khan et al. [22] research the principles of deep learning (DL), specifically neural networks and convolutional neural networks, and how they are

used in natural language processing (NLP). The research looked into new developments, difficulties, and trends in DL and NLP. The research found that although deep learning models are quite good at certain tasks, like natural language processing (NLP), they have trouble comprehending pragmatic parts of language because they rely too much on statistical learning methods. It gave insights into the most recent cutting-edge developments in DL and NLP as well as important roadblocks. Complex features and unbalanced data make intrusion detection in network traffic difficult. To tackle imbalanced network traffic, Farhan Ullah's research suggests an IDS based on transformer-based transfer learning. In order to research IDS-INT and address data imbalance using SMOTE, Farhan Ullah et al. [23] used transformer-based transfer learning to comprehend feature interactions in network traffic. For assault detection, they used a hybrid CNN-LSTM model. Using benchmark datasets, the suggested IDS-INT method was evaluated and shown to be successful in identifying a range of threats. For model interpretation and trust-building, an explainable AI technique was used. Looked at data mining for social media on Android, identifying trends and knowledge gaps Hou ssem Lahiani et al. [24]. A thorough analysis was conducted to look at themes, techniques, and challenges in research published between 2015 and 2022. According to the report, data mining for images and videos was given less attention than that for text and machine learning. Further insights on ethics and privacy were noted, and they will direct future directions in the field. A major problem posed by the proliferation of security-related attacks on Internet-of-Things (IoT) devices is their exponential expansion. In order to find security flaws in IoT systems and provide workable fixes, simulations of ethical hacking are suggested. Jean-Paul A. Yaacoub et al. [25] used ethical hacking techniques and instruments to investigate both the technical and non-technical elements of security flaws in IoT devices. The focus was on conducting frequent penetration testing and simulations at different IoT infrastructure levels in order to assess risks and identify exploitable flaws. Researchers found that IoT security flaws and vulnerabilities might be found with the use of ethical hacking simulators. IoT settings' overall security posture was improved by proposing and adopting workable security solutions based on risk assessments and simulated assaults.

Previous research on the identification of spam and phishing encountered difficulties such poor detection rates, vulnerability to evasion strategies, and insufficient precision. Future research should include sophisticated machine learning models, such as Support Vector Machines (SVM), LightGBM, and hybrid deep learning architectures, to address these issues and provide more reliable spam identification in emails and SMS. Furthermore, investigating integrated frameworks can improve the security of Internet of Things (IoT) sensor networks. One example of this is the combination of blockchain technology and machine learning. Technologies like explainable AI and simulations of ethical hacking provide viable ways to fix security holes in Internet of Things devices. Innovative methods, such as a hybrid correlation-based deep learning model for spam email classification, and ongoing machine learning algorithm advancements can help increase the efficacy and precision of cyber threat identification.

3. Components of the Enhanced Framework

The upgraded SMS spam detection framework combines blockchain technology and machine learning algorithms to build a powerful and transparent approach for battling SMS spam. At its heart, the framework is made up of multiple interrelated components. To begin, raw SMS data is collected from multiple sources and pre-processed before being analysed further. Next, feature extraction algorithms are used to extract useful information from SMS messages, including text content, sender information, and metadata. These characteristics are used as inputs to machine learning algorithms that determine whether SMS messages are spam or authentic. The machine learning models are trained on labelled datasets and updated on a regular basis to keep up with changing spam strategies. Furthermore, the framework makes use of blockchain technology to provide secure SMS data storage and validation. By keeping transaction records on a decentralised and immutable ledger, the architecture assures the spam detection process's integrity and transparency. Smart contracts provide automatic verification and validation of SMS data, increasing the framework's efficiency and dependability.

3.1 Evaluation Of Machine Learning Algorithms

Several criteria must be addressed while assessing machine learning algorithms for SMS spam detection within the context of the suggested

framework to achieve optimal performance. Although decision trees are interpretable and easy to grasp, they may struggle with complicated decision boundaries. Support vector machines thrive in high-dimensional feature spaces, are resistant to overfitting, and may be computationally costly. While neural networks are effective at catching subtle patterns, they need a significant amount of data and computer resources to train. The assessment includes evaluating algorithm performance indicators including accuracy, precision, recall, and F1-score, as well as computing economy and scalability. Cross-validation and hyperparameter tweaking are also used to optimise algorithm performance. Finally, the chosen algorithm should strike a balance between accuracy, efficiency, and scalability in order to properly identify between spam and authentic SMS messages in real-time processing circumstances.

3.2 Blockchain Integration And Security Considerations

Integrating blockchain technology into the SMS spam detection framework brings a number of security issues that are critical to its effectiveness. Blockchain's decentralised and irreversible nature provides natural advantages in terms of data integrity and transparency. However, ensuring strong security necessitates careful consideration of several elements. To begin, adopting proper consensus methods, like as proof of labour or proof of stake, is critical to preventing bad actors from interfering with the blockchain. Furthermore, integrating smart contracts to manage interactions and enforce rules inside the framework improves automation while lowering the chance of human mistake. Furthermore, preserving data privacy is critical, which necessitates the encryption of sensitive information and the implementation of access control systems to prevent unauthorised access. Furthermore, resolving possible weaknesses, such as 51% assaults or double-spending, necessitates proactive steps such as network monitoring and security protocol implementation.

Data Transformation For Analysis

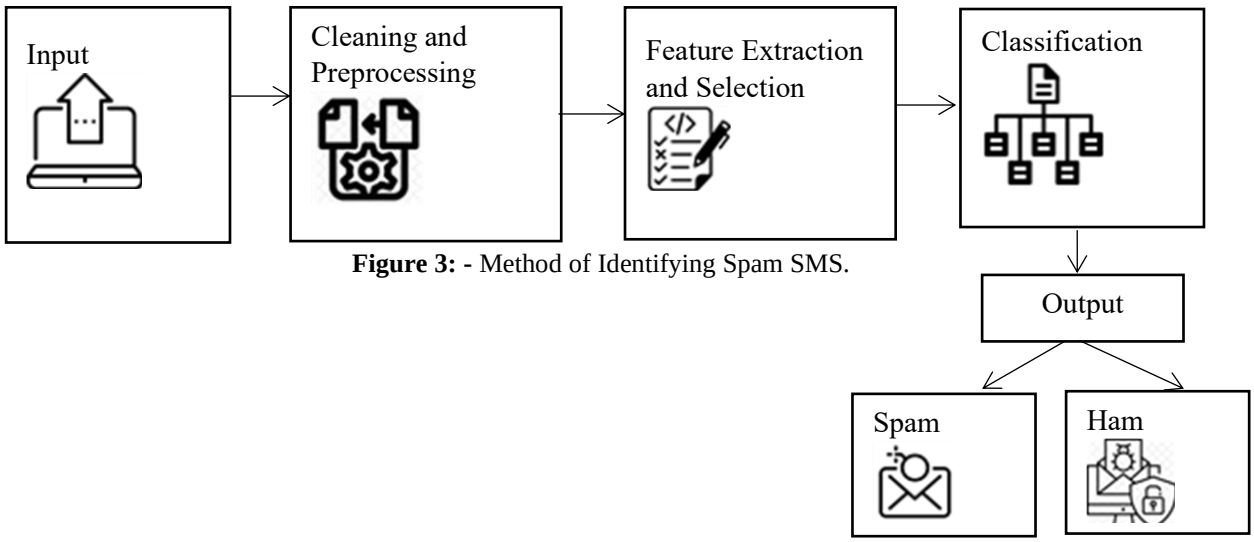


Figure 3: - Method of Identifying Spam SMS.

The suggested approach for classifying SMS messages starts with the raw messages being cleaned and pre-processed. Next, pertinent features are extracted using TFIDF. The Random Forest classifier is used due to its resilience, and feature selection is used to improve model performance. By classifying each message as "Spam" or "Ham," the classification method' output offers a useful way to differentiate between spam and legitimate SMS communications. By ensuring that the model can manage intricate relationships in the data, this sequential flow maximizes the accuracy of SMS message categorization as shown in figure 3.

4. Challenges

- **Integration Complexity**: Balancing blockchain's openness with ML's predictive capacity necessitates sophisticated synchronisation to ensure effective data transit between blockchain components and ML models.
- **Scalability:** Balancing blockchain's immutable record with ML's computing needs is a hurdle,

demanding novel methods to handle growing SMS volumes and blockchain size.

- **Security and Privacy:** Protecting user data on a public ledger raises privacy issues, necessitating strong encryption and access restrictions while adhering to data protection laws.
- **Adaptability to Emerging Spam Techniques:** To successfully tackle growing threats, it is necessary to constantly update models and enhance features in order to stay ahead of dynamic spam methods.
- **Regulatory Compliance:** Maintaining a balance between blockchain's decentralised nature and regulatory obligations necessitates strict adherence to data protection and telecommunications standards, as well as clear user consent methods and legal frameworks.

5. Advantages

An improved SMS spam detection system that incorporates blockchain and machine learning has numerous appealing benefits. To begin, by using blockchain technology, the system improves transparency and immutability in spam detection procedures. SMS spam detection actions are publicly documented because to blockchain's decentralised ledger, which provides auditable trails of detection and categorization choices. This openness, which provides visibility into how spam messages are recognised and controlled, helps build confidence among stakeholders such as telecommunications regulators, service providers, and end users.

Second, by combining blockchain with machine learning, the framework can take use of the benefits of both technologies, resulting in more powerful spam detection. Machine learning algorithms can analyse enormous amounts of SMS data to detect spam trends, while blockchain maintains the data's integrity and confidentiality. Furthermore, blockchain can enable the secure sharing of spam-related data among diverse entities while maintaining anonymity, allowing for effective joint efforts to combat SMS spam. Overall, this improved methodology shows promise for more transparent, safe, and effective SMS spam detection, which will benefit both telecoms sector stakeholders and end-users.

6. Disadvantages

While an improved SMS spam detection system that uses blockchain and machine learning has various benefits, it also has considerable drawbacks. For starters, the difficulty of integrating blockchain and machine learning systems might be challenging. Combining these technologies necessitates sophisticated synchronisation methods to assure continuous connection and data sharing, thereby increasing development time and complexity. Furthermore, the intrinsic properties of blockchain technology may restrict the framework's scalability. Blockchain's consensus methods and data storage needs may limit the system's capacity to handle enormous volumes of SMS messages in real time, resulting in latency concerns and degraded performance.

Furthermore, the security and privacy implications of keeping SMS data on a public blockchain raise serious issues. While blockchain provides immutability and transparency, it also exposes critical SMS content to everyone who has access to the blockchain, increasing privacy hazards. Ensuring strong encryption and access restrictions is critical for protecting user data, but these measures may add complexity and overhead. Furthermore, regulatory compliance is a substantial barrier because the framework must manage data protection rules and telecommunications regulations while utilising decentralised technology. Achieving compliance while retaining the blockchain's integrity and openness complicates the framework and increases its potential downsides.

7. Features

- **Blockchain Transparency:** Spam detection records are stored using blockchain's transparent and immutable ledger, ensuring transparency and auditability of spam detection actions.
- **Machine Learning Algorithms:** Advanced machine learning algorithms are used to analyse SMS content and metadata, allowing for effective spam identification while reducing false positives.
- **Decentralised Reputation System:** Uses a blockchain-based decentralised reputation system to award trust ratings to SMS senders based on their previous behaviour, which aids in spam categorization and filtering.
- **Smart Contracts:** Smart contracts are used to automate interactions and enforce rules within the framework, allowing for safe and trustless transactions between network members while also assuring integrity in spam detection procedures.
- **Data Privacy Measures:** Uses encryption and privacy-preserving measures to secure user privacy and sensitive information, guaranteeing compliance

with data protection standards while taking use of blockchain's transparency and security characteristics.

8. Future Scope

Future SMS spam detection research intends to improve accuracy and efficiency by refining machine learning algorithms, optimising blockchain integration, and exploring new technologies such as federated learning and differential privacy. The focus will be on fine-tuning models for precision while minimising computational costs, assuring scalability for real-world application. Integrating with messaging systems other than SMS and using decentralised reputation systems can improve usability and efficacy across all channels. Real-time user feedback systems, as well as training ML models on varied datasets, seek to increase reliability and handle issues such as recognising slang and non-English languages. Exploring approaches such as Information Gain and Gini Index, as well as including contextual data such as sender name and message frequency, might help to improve SMS spam detection capabilities.

9. Conclusion

The combination of machine learning (ML) with blockchain technology offers a viable path to improving security in a variety of fields, including mobile communication services like SMS. While blockchain provides intrinsic security through its immutable ledger and built-in encryption, machine learning (ML) adds powerful analytics and predictive capabilities. However, despite a growing amount of research on the security implications of machine learning and blockchain, significant issues remain, including scalability, interoperability, privacy concerns, and vulnerability to adversarial attacks. Nonetheless, recent breakthroughs like as federated learning and zero-knowledge proofs provide hope for overcoming these difficulties. Moving forward, future research should prioritise privacy-preserving approaches, improve ML algorithm efficacy and scalability, and investigate the integration of other cutting-edge technologies with ML and blockchain to develop innovative solutions for combating spam and improving security in mobile communication services. Our experiments show that ML classifiers like Support Vector Machine, K-Nearest Neighbour, and Naïve Bayes are successful in detecting spam. Support Vector Machine is the best choice based on metrics like accuracy, precision, recall, and F-score. These findings highlight the potential for ML-powered ways to improve SMS security and pave the way for future mobile communication systems that are safer and more efficient

References

[1] Ashfaq, T.; Khalid, R.; Yahaya, A.S.; Aslam, S.; Azar, A.T.; Alsafari, S.; Hameed, I.A. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors 2022, 22, 7162. https://doi.org/10.3390/s22197162

[2] [Livingston Jeeva, Ijtaba Saleem Khan (2023), A Review Article On Enhancing Email Spam Filter's Accuracy Using Machine Learning, International Journal of Innovative Research in Computer Science and Technology (IJIRCST), Vol-11, Issue-4, Page No-5-11], (ISSN 2347 - 5552). www.ijircst.org

[3] Ahmed, Naeem & Amin, Rashid & Aldabbas, Hamza & Koundal, Deepika & Alouffi, Bader & Shah, Tariq. (2022). Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges. Security and Communication Networks. 2022. 10.1155/2022/1862888.

[4] Aaisha Makkar, Neeraj Kumar,An efficient deep learning-based scheme for web spam detection in IoT environment,Future Generation Computer Systems,Volume 108,2020,Pages 467-487,ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.03.004.

[5] Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar,Artificial intelligence for cybersecurity: Literature review and future research directions,Information Fusion,Volume97,2023,101804,ISSN15662535, https://doi.org/10.1016/j.inffus.2023.101804.

[6] Kaddoura S, Chandrasekaran G, Elena Popescu D, Duraisamy JH. A systematic literature review on spam content detection and classification. PeerJ Comput Sci. 2022 Jan 20;8:e830. doi: 10.7717/peerj-cs.830.

[7] A. Saxena, R. Taluja, M. Sararswat, N. Shalini, O. Krishna and P. Kumar, "Data Mining Methods for Internet of Things: A Survey," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 2610-2618, doi: 10.1109/IC3I59117.2023.10397668.

[8] Nallamothu, P. T., & Khan, M. S. (2023). Machine Learning for SPAM Detection. Asian Journal of Advances in Research, 6(1), 167–179. Retrieved from https://www.mbimph.com/index.php/AJOAIR/article/view/3417.

[9] Ghourabi, A.; Alohaly, M. Enhancing Spam Message Classification and Detection Using Transformer-Based Embedding and Ensemble Learning. Sensors 2023, 23, 3861. https://doi.org/10.3390/s23083861.

[10] Bazzaz Abkenar S, Haghi Kashani M, Akbari M and Mahdipour E. (2023). Learning textual features for Twitter spam detection. Expert Systems with Applications: An International Journal. 228:C. Online publication date: 15-Oct-2023. https://doi.org/10.1016/j.eswa.2023.120366.

[11] Umair Maqsood, Saif Ur Rehman, Tariq Ali, Khalid Mahmood, Tahani Alsaedi, Mahwish Kundi, "An Intelligent Framework Based on Deep Learning for SMS and e-mail Spam Detection", Applied Computational Intelligence and Soft Computing, vol. 2023, Article ID 6648970, 16 pages, 2023. https://doi.org/10.1155/2023/6648970.

[12] Shereen Ismail, Muhammad Nouman, Diana W. Dawoud, Hassan Reza, Towards a lightweight security framework using blockchain and machine learning, Blockchain: Research and Applications, 2023, 100174, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2023.100174.

[13] H. A. Al-Kabbi, M. -R. Feizi-Derakhshi and S. Pashazadeh, "Multi-Type Feature Extraction and Early Fusion Framework for SMS Spam Detection," in IEEE Access, vol. 11, pp. 123756-123765,2023, doi: 10.1109/ACCESS.2023.3327897

[14] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, Jari Porras, Mitigation strategies against the phishing attacks: A systematic literature review, Computers & Security, Volume 132, 2023, 103387, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103387.

[15] Enrique Cano-Marin, Marçal Mora-Cantallops, Salvador Sanchez-Alonso, The power of big data analytics over fake news: A scientometric review of Twitter as a predictive system in healthcare, Technological Forecasting and Social Change, Volume 190, 2023, 122386, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2023.122386.

[16] Ahsan Nazir, Jingsha He, Nafei Zhu, Ahsan Wajahat, Faheem Ullah, Sirajuddin Qureshi, Xiangjun Ma, Muhammad Salman Pathan, Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration, Journal of King Saud University - Computer and Information Sciences, Volume 36, Issue 2, 2024, 101939, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2024.101939.

[17] Claudia Durán, Christian Fernández-Campusano, Raúl Carrasco, Eduardo Carrillo, DMLBC: Dependable machine learning for seaports using blockchain technology, Journal of King Saud University - Computer and Information Sciences, Volume 36, Issue 1, 2024, 101918, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2024.101918.

[18] Salman, Muhammad & Ikram, Muhammad & Kaafar, Dali. (2024). Investigating Evasive Techniques in SMS Spam Filtering: A Comparative Analysis of Machine Learning Models. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3364671. DOI:10.1109/ACCESS.2024.3364671

[19] Ahsan Wajahat, Jingsha He, Nafei Zhu, Tariq Mahmood, Ahsan Nazir, Faheem Ullah, Sirajuddin Qureshi, Soumyabrata Dev, Securing Android IoT devices with GuardDroid transparent and lightweight malware detection, Ain Shams Engineering Journal, 2024, 102642, ISSN 2090-4479, https://doi.org/10.1016/j.asej.2024.102642.

[20] Christoph Gehweiler, Oleg Lobachev, Classification of intent in moderating online discussions: An empirical evaluation, Decision Analytics Journal, Volume 10, 2024, 100418, ISSN 2772-6622, https://doi.org/10.1016/j.dajour.2024.100418.

[21] Femi Emmanuel Ayo, Lukman Adebayo Ogundele, Solanke Olakunle, Joseph Bamidele Awotunde, Funmilayo A. Kasali, A hybrid correlation-based deep learning model for email spam classification using fuzzy inference system, Decision Analytics Journal, Volume 10, 2024, 100390, ISSN 2772-6622, https://doi.org/10.1016/j.dajour.2023.100390.

[22] Wahab Khan, Ali Daud, Khairullah Khan, Shakoor Muhammad, Rafiul Haq, Exploring the frontiers of deep learning and natural language processing: A comprehensive overview of key challenges and emerging trends, Natural Language Processing Journal, Volume 4, 2023, 100026, ISSN 2949-7191, https://doi.org/10.1016/j.nlp.2023.100026.

[23] Farhan Ullah, Shamsher Ullah, Gautam Srivastava, Jerry Chun-Wei Lin, IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic, Digital Communications and Networks, 2023, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2023.03.008.

[24] Houssem Lahiani, Mondher Frikha, A Systematic Review of Social Media Data Mining on Android, Procedia Computer Science, Volume 225, 2023, Pages 2018-2027, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.10.192.

[25] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Ali Chehab, Ethical hacking for IoT: Security issues, challenges, solutions and recommendations, Internet of Things and Cyber-Physical Systems, Volume 3, 2023, Pages 280-308, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2023.04.002.