Neighbor Spoofing in Spam Calls: Cybersecurity Risks and Effective Defense Mechanisms

Andi Kesya Claproth [1, *], Aminah Kaitlyn Latifah [2], Yohan Muliono [3], Ika Dyah Agustia Rachmawati [4]
[1, 2, 3, 4] Cyber Security Department, Bina Nusantara University, Jakarta, Indonesia
Email: [1,*] andi.claproth@binus.ac.id, [2] aminah.latifah@binus.ac.id, [3] ymuliono@binus.edu, [4] ika.rachmawati001@binus.ac.id
*Corresponding Author

Abstract—**Neighbor spoofing in spam calls, where attackers mimic local phone numbers to increase response rates, poses significant privacy and security risks. In Indonesia, spam calls surged to 25.8 million in January 2021, with users receiving an average of 14 spam calls monthly. Using a qualitative approach, this study explores the impact of neighbor spoofing and evaluates the effectiveness of defense mechanisms, specifically the STIR/SHAKEN protocol, in the Indonesian telecommunications context. Findings indicate that while STIR/SHAKEN offers promising potential to reduce spoofing, its adoption faces challenges, with only 17% of telecom providers fully implementing it, 27% partially implementing it, and 56% relying on alternative methods. This study proposes strategic recommendations to enhance user trust and strengthen defenses against the pervasive threat of neighbor spoofing in spam calls.**

Keywords—Spam Calls, Caller ID, Neighbor Spoofing, STIR/SHAKEN, Robocall, telecommunications security

I. INTRODUCTION

Information and communication technology play a crucial role in life. Technology helps people conduct productive activities efficiently. Work, economy, transportation, and health all improved. These areas became more integrated. Individuals functioned more effectively because of it. The Internet was one key part of this tech. The Internet interconnects networking computers into a network of computers. It integrated various networks across the globe. Territorial, legal, or cultural boundaries[1]. This made sharing information more effortless than ever before. In 1969, ARPANET launched as the first version of the Internet. Also, email emerged shortly after that in the 1970s. It changed how people communicated instantly across distances-websites followed in the 1990s with Tim Berners-Lee's invention of the World Wide Web. More so, social media platforms like Facebook and Twitter appeared in 2004 and 2006, respectively. They transformed personal interactions into public exchanges. Yet challenges arose, too, due to misinformation spreading online quickly during events like elections or crises. Nevertheless, technology continued evolving rapidly over time, shaping modern society significantly. Technology has a lasting impact on daily life and communication methods worldwide, changing how individuals connect forever.

In 2024, Indonesia saw a significant rise in internet usage. The Association of Indonesian Internet Service Providers reported 221,563,479 internet users out of a total population of 278,696,200 in 2023. This was a notable increase. The internet penetration rate hit 79.5%. It marked a growth of 1.4% from before. The data demonstrates how significant the role of the internet has become in daily life. People relied on it more than ever for communication and information. Also, businesses thrived online due to this trend. More so, education shifted towards digital platforms during this time. This shift had both positive and negative effects. On the one hand, access to information has significantly expanded. On the other hand, issues like false data emerged as concerns grew about misinformation spreading rapidly online. Overall, increased internet usage significantly shaped society in Indonesia by enhancing connectivity and introducing challenges that needed addressing moving forward.

The internet transformed the economy forever. It became an integral part of economic activities, and financial players utilized this technology to optimize processes. E-commerce emerged as a significant application of the Internet. Producers and consumers interact online without face-to-face meetings, making conducting transactions more straightforward and more efficient. Digital platforms also help businesses connect with consumers effectively. Technological advancements have made communication more effective and efficient [2].

Table 1

Total usage of e-commerce applications in indonesia in 2023

No	*Year*	*Number of Users (Millions)*
1	*2020*	*38.72*
2	*2021*	*44.43*
3	*2022*	*50.89*
4	*2023*	*58.63*

The data in Table 1 demonstrates a significant annual increase in the number of e-commerce application users in Indonesia. In 2020, the user count recorded 38.72 million. It rose significantly. In 2021, it reached 44.43 million. Then, in 2022, it will increase to 50.89 million. By 2023, e-commerce users in Indonesia grew to 58.63 million. This data reflects a consistent growth pattern in e-commerce use. More so, it matched the rise of digital tech adoption among Indonesians. E-commerce has played a vital role in supporting consumer needs across various economic sectors. The increase in users reflected changing shopping habits and preferences as people

Received: 24-1-2025
Revised: 20-7-2025
Published: 31-12-2025

turned more to online platforms for purchases. The impact was substantial on local businesses and consumers alike. Many small shops moved online to reach wider audiences while consumers enjoyed convenience and variety at their fingertips. This shift also brought challenges like competition and logistics issues but ultimately led to innovation within the market. Overall, this growth profoundly shaped Indonesia's economic landscape over the years, creating a legacy of increased accessibility and choice for consumers while supporting business development across various industries[3].

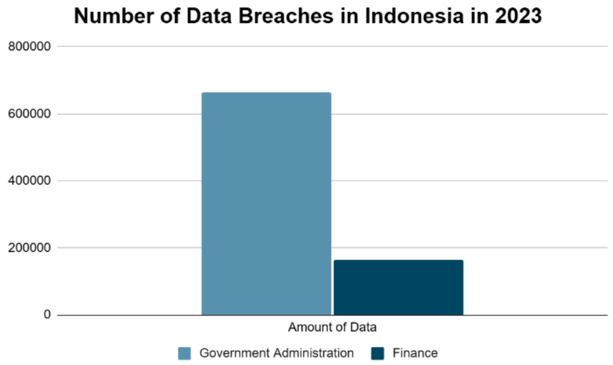

Fig 1. Number of Data Breaches During 2023

The rise of e-commerce brought many users. Yet, it also led to more security threats, as sensitive information became increasingly vulnerable. Names, addresses, and identification numbers (NIK) were stored in these applications, along with credit card information and transaction histories. Spam calls became a significant issue, with Caller ID spoofing as a common tactic. In Indonesia, spam calls spiked dramatically in January 2021, reaching 25.8 million calls, with each user facing an average of 14 spam calls monthly. This situation highlighted the security threats associated with online shopping[3].

Data breaches further exacerbated these concerns. In 2023 alone, Indonesia experienced significant data leaks, with over 600,000 data breaches occurring in government administration sectors and a substantial amount in the finance sector. This alarming number of breaches emphasizes the need for stronger security measures to protect personal data from misuse and exploitation as e-commerce and digital activities expand.

Cybercriminals exploited data to call users. They pretended to know them by citing gathered information. This strategy helped criminals gain victims' trust quickly. Caller ID spoofing led to another crime: voice manipulation. AI technology advancements and scammers' voices. They could sound like close relatives or official institution representatives. This voice manipulation played a crucial element in telephone scams-phishing tactics. Scammers created scenarios that are more convincing than email or web-based phishing methods. The impact was significant; many fell victim to these tricks over time. In 2021, the Federal Trade Commission reported a rise in such scams. Victims lost millions of dollars due to these deceptive practices. Awareness became essential for combating this issue. The long-term effects of these crimes were significant, too. Trust in phone communications diminished significantly as people became more cautious about unknown calls. Cybercriminals have left a lasting mark on society through their actions and tactics. The evolution of technology has enabled new ways for them to exploit individuals, changing how people interact with each other on the phone forevermore[4].

Therefore, this paper aims to explore the security risks posed by the neighbor spoofing technique in spam calls and evaluate effective defense mechanisms to protect users from these threats. We also hope to provide strategic recommendations to minimize the negative impact of neighbor spoofing practices in spam calls.

II. Literature Review

A. Spam Calls and Their Impact in Indonesia

In 2021, Indonesia faced a significant rise in spam calls. Research by Global Spam showed it was one of the 20 countries with the highest spam call rates. Each person gets around 14 spam calls every month[3]. Truecaller, a caller ID app company, found that half of its users in Indonesia received calls from unknown numbers. The experience continued in 2023, with more robocalls appearing everywhere, including the in United States. Spam calls became a common nuisance for many individuals. These unwanted interruptions led to frustration and concern about privacy. Some individuals made efforts by using apps to block these calls or report them. Yet, despite efforts, the problem persisted. The impact of these spam calls extended beyond nuisance. They extended concern among users about potential scams and scams linked to these unknown callers. Awareness grew as more individuals shared their experiences online. The long-term effects of this surge were significant. It changed how individuals viewed telecommunications and trust in technology. More so, it pushed companies to improve their services against such threats. Indonesia's experience with spam calls reflects broader global trends in telecommunications challenges today[5].

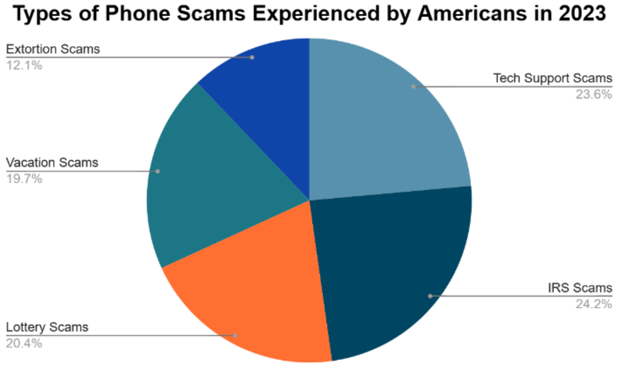

Fig 2. Distribution of Common Phone Scams Targeting Americans in 2023

B. Robocalls, Caller ID Spoofing, and Global Concerns

According to research by WhistleOut, there was a 7% rise in robocalls in the U.S., which jumped from 49 billion to 53 billion in just one year. These robocalls include various types. They included spam, telemarketing, fraudand debt collection. This led to significant financial losses for consumers. Many of these robocalls were also spam.

Consumers often receive unwanted or harmful robocalls. WhistleOut data (Chart 2) indicates some of the most common phone scams. Tech support scams made up 37%. IRS scams followed at 33%. Lottery scams accounted for 32%. Vacation scams were at 31%, while extortion reached 19%. The impact was clear and troubling. Robocalls created confusion and fear among people. Therefore, many sought ways to block them but faced challenges with technology and regulations. The increase in these robocalls raised privacy concerns as well. The rise of robocalls represented a significant issue affecting many Americans' daily lives and finances. The long-term effects could shape how people interact with their phones moving forward. The FCC urges. Consumers faced fraudulent spam calls and robocalls. Reporting these incidents to the FCC Consumer Complaint Center was crucial. It helped with investigations and enforcement efforts. Yet, the trend persisted. Robocalls and spam calls continued to pose a serious threat. Public safety suffered because of this issue. Financial security was at risk, too[6]. The ongoing control efforts seemed ineffective in curbing these nuisances. More people were annoyed despite the measures in place. This highlighted a growing concern in society about communication safety.

Spam calls are intrusive in daily life. These unwanted calls are aimed at marketing or promotions. Sometimes, they conducted fraudulent intentions. In 2020, the volume of spam calls surged dramatically. Many people received these calls without the recipients' consent. Robocalls became automatic as technology advanced. Also, perpetrators often used Caller ID spoofing techniques. This made their calls appear more credible than they were. The tactics confused many recipients and led to increased fear of scams. More so, some individuals fell victim to these schemes. The impact was widespread and troubling. People lost money and trust in phone communications. Efforts to combat spam calls began around the early 2000s but faced challenges due to evolving technology. Nevertheless, awareness grew over time about the dangers of spam calls. Many sought efforts to combat them or report fraudulent activity. Overall, spam calls highlighted significant issues in telecommunications that needed addressing. Spam calls have impacted society's view of phone safety, and privacy concerns still exist today[7].

C. *Efforts to Combat Spam Calls and Technological Solutions*

Caller ID manipulation is a tactic used to deceive people. It involved falsifying the displayed number or identity to appear trustworthy. Local numbers or familiar company names are often used. This method made it easier for spam call operators to get answers. Recipients might think the call was from a reliable source. The Caller ID feature was meant to help identify callers but exploited deception instead. This technique had significant implications. Trust in phone communication decreased over time. Many people felt anxious about answering calls from unknown numbers. Spam call operators took advantage of this trust issue, increasing frustration among recipients. In 2020, legislation aimed at combating these practices emerged in the U.S., yet challenges remained in enforcement and enforcement. More so, technology continued evolving, allowing scammers to adapt their methods swiftly. The long-term implications of this manipulation were significant. Trust in phone communication eroded further as awareness grew about these tactics. People became more anxious when answering calls, highlighting legitimate businesses, too. Ultimately, this situation highlighted the need for better security measures and education on recognizing scams. Awareness campaigns emerged as a response to these issues, aiming to protect consumers from falling victim to such tactics in the future[7].

Caller ID spoofing became a growing concern. Spam calls and robocalls flooded phone lines. In response, technological solutions emerged to tackle the problem. The STIR/SHAKEN protocol was one of the primary solutions proposed. It specifically designed caller identity spoofing in telecommunications networks. This protocol worked by authenticating caller identities using digital certificates from trusted authorities. Telecommunications operators could then verify the legitimacy of caller identities[8]. Also, this approach helped reduce fake calls significantly. However, challenges remained in full implementation across all networks. Some smaller providers struggled with adopting the technology due to costs and complexity. Nevertheless, larger companies began integrating STIR/SHAKEN into their systems. Further developments were necessary for widespread effectiveness against spam calls and robocalls. The collaboration between various stakeholders proved essential for success in combating this issue. While STIR/SHAKEN represented progress against Caller ID spoofing, ongoing efforts were needed to resolve the problem in telecommunications.

Telecom service providers had a new protocol. This protocol helped them detect and block suspicious calls. It worked before the calls reached consumers. The goal was to protect people from fraud and protect personal personal data. However, the implementation of this protocol varied among companies. Only 17% of telecom companies fully implemented STIR/SHAKEN technology. That number represented 536 companies in total. A more significant portion, 27%, partially implemented it, which meant 817 companies were still adopted. Yet, a considerable majority, about 56%, or 1,710 companies, had not adopted it. They relied on robocall mitigation methods instead. The impact of STIR/SHAKEN was noticeable after its rollout. Data from YouMail revealed that robocalls in the United States decreased by 29%. This decrease occurred between June and August of 2021[9]. The numbers indicated a positive impact from using this technology[10]. While some progress was made with STIR/SHAKEN adoption, many telecom providers have ongoing challenges in full implementation. The initial results indicated progress in reducing suspicious calls but highlighted ongoing challenges in widespread adoption across the industry.

Verizon was one of the largest operators. It reported blocking over 13 billion unwanted calls. This happened by utilizing analytics to identify robocall sources. The company aimed to reduce robocalls significantly. Around 500 million calls were reduced each month. Analytics helped identify the sources of these annoying calls. Also, this move showed Verizon's commitment to customer service[9]. Robocalls have become a big problem for many users. People were frustrated with constant interruptions from spam calls. Therefore, taking action was necessary. In 2020, the Federal

Communications Commission took steps against robocalls, too. They implemented new rules to help protect consumers from[10].

III. Methodology

A. Comparative Analysis Through Literature Review

This study includes an in-depth literature review of academic papers, industry reports, and related studies to compare STIR/SHAKEN with other robocall mitigation methods, such as call-blocking applications and machine learning technology. The review provides insights into:

- The advantages, disadvantages, and challenges of implementing various solutions
- Case studies on the implementation of STIR/SHAKEN by major operators to analyze real-world effectiveness

The data collected from these papers shows that STIR/SHAKEN technology has significantly reduced the number of spoofing and robocalls. Although imperfect, the protocol enables the detection and blocking of suspicious calls, increases consumer transparency through a "possible scam" warning, and assists authorities in tracking robocall perpetrators via a digital trail recorded within the network. The table shows that the majority of respondents feel highly disturbed by the frequency of spam calls they receive and are dissatisfied with the effectiveness of current blocking technologies. Most respondents also express a lack of trust in the Caller ID feature due to frequent spoofing that makes the caller's identity unreliable.

This study will also include an in-depth literature review of academic journals, industry reports, and related articles to compare STIR/SHAKEN with other robocall mitigation methods, such as call-blocking applications and machine learning technology. This literature review will comprehensively overview various solutions' advantages, disadvantages, and challenges. Additionally, case studies on the implementation of STIR/SHAKEN by major operators will be analyzed to understand the real-world effectiveness of this protocol. According to data, STIR/SHAKEN technology has shown a significant reduction in the number of spoofing and robocalls. Moreover, STIR/SHAKEN helps authorities track and take action against robocall perpetrators through a digital trail recorded within the network.

B. Mechanism, Implementation, and Policy Challenges of STIR/SHAKEN

STIR/SHAKEN verifies the caller's identity to prevent Caller ID spoofing. When a malicious caller initiates a call, the carrier logs the entry point, identifying the device and location where the call enters the network. The caller's carrier then assigns an attestation level (A, B, or C) to the call based on the level of confidence in the caller's authenticity, with level "A" indicating high confidence and "C" indicating low confidence. The carrier encrypts the caller's identity information, including the attestation level, and transmits it along with the call to the recipient's carrier. The recipient's carrier uses the attestation level, previous records, and complaints associated with similar network entry points to assess the call's legitimacy. If the call is suspected to be fraudulent, a warning such as "possible scam" is displayed on the recipient's Caller ID. The recipient can ignore or report the call, assisting carriers and authorities in tracking robocall perpetrators. This digital trail enables the recipient's carrier and regulatory authorities to trace the call to its origin, facilitating legal action against robocalls.

An evaluation of policies and the compliance level of operators with FCC regulations will also be conducted to see how government regulations play a role in encouraging the adoption of this technology in the United States. However, challenges in implementing STIR/SHAKEN remain, especially in international telecommunications networks and legacy networks that do not yet support this technology. Further development of this protocol includes expanding to broader networks and adapting it to be more compatible with older or international networks. This methodology is expected to provide a comprehensive understanding of STIR/SHAKEN's effectiveness in reducing the threat of robocalls and spoofing, and the challenges that must be addressed to achieve broader success.

IV. RESULT

A. The Escalating Threat of Neighbor Spoofing

The problem has become so pervasive that it threatens user privacy and trust in Caller ID systems worldwide. There are many attacks in which the attackers disguise their calls with local, or at least familiar-looking, phone numbers to take advantage of user trust in recognizing numbers from their area. In Indonesia, the scale of neighbor spoofing is alarming. In January 2021, spam calls through neighbor spoofing reached as many as 25.8 million, accounting for an average of 14 calls per user in one month. This is a considerable increase compared to the previous years, showing how sophisticated and effective spoofing methodologies have become to deceive users. The prevalence of neighbor spoofing is compounded by the now-growing number of data breaches that supply attackers with personal information to make these spoofed calls appear legitimate. Indonesia, for example, noted 600,000 data breaches in 2023 alone, mainly targeting sensitive sectors of government, finance, and e-commerce. These breaches supplied attackers with names, phone numbers, and other personal details, making the neighbor spoofing scheme more credible and difficult for recipients to detect.

This trend strongly correlates with Indonesia's growing internet penetration. By 2023, 221.5 million users were connected to the internet, achieving an internet penetration rate of 79.5%, up 1.4% from the previous year. While digital connectivity fosters economic growth and communication, it also opens up vulnerabilities to cyber and telecommunication threats like neighbor spoofing. The data below highlights the relationship between spam call trends, data breaches, and internet penetration rates.

Table 2

Internet usage growth and security threats in indonesia (2020-2023)

Year	Spam Calls (Millions)	Avg. Spam Calls per User	Data Breaches (Cases)	Internet Penetration (%)
2020	18.500.000	12	350.000	75.1%
2021	25.800.000	14	450.000	76.9%
2022	22.000.000	13	550.000	78.1%
2023	28.000.000	15	600.000	79.5%

The sharp increase in spam calls from 18.5 million in 2020 to 28 million in 2023, combined with rising internet usage, demonstrates the growing scale of the problem. Neighbor spoofing undermines public confidence in telecommunication systems and highlights the urgent need for robust measures like STIR/SHAKEN to combat these threats effectively.

B. *Effectiveness of STIR/SHAKEN in Combating Neighbor Spoofing*

STIR/SHAKEN has a promising prospect of preventing neighbor spoofing by verifying the authenticity of caller IDs through digital certificates issued by trusted authorities. This technology blocks illegitimate calls and enhances transparency by allowing users to see warnings, such as "possible scam," on their Caller IDs. Success has been witnessed with STIR/SHAKEN in countries such as the United States, where, within the first three months of its implementation, robocalls fell 29%. This demonstrates that it effectively detects and mitigates spoofed Caller IDs, reducing users' exposure to fraudulent schemes. In Indonesia, however, the adoption of STIR/SHAKEN is uneven and partial. Fully implemented by only 17% of the providers in 2023 and partially adopted by another 27%, a whopping 56% of providers continue to use less effective measures. Thus, most of the population would still be vulnerable to spoofing and robocalling. This is where less-than-extensive implementation does not let the protocol explore its full potential for addressing neighbor spoofing and undermines public trust in telecommunication systems. This incessant threat of fraudulent activities will make users increasingly wary of answering calls.

It is, therefore, difficult for Indonesia to adopt due to high costs, where most of the smaller providers cannot afford infrastructure upgrading for implementation. The integration of STIR/SHAKEN into the existing system is very technical and complicated, with particular reference to legacy networks and international calls. This problem worsens because of certain regulatory loopholes, such as the fact that no policy drives the implementation of this protocol all over the nation. Without enforcement, telecommunications providers have little urgency to implement the key technology.

Addressing such challenges will significantly contribute to realizing full STIR/SHAKEN functionality in Indonesia. Providing incentives in the form of subsidies or tax breaks may convince small operators to invest in this infrastructure. Government regulations and severe laws have a significant role to play in ensuring all providers apply this protocol uniformly as one way of tackling spoofing. This calls for cooperation between regulators and the telecommunication industry in producing solutions that allow STIR/SHAKEN to work on different network systems nationally and internationally. If implemented, Indonesia can considerably reduce the threats of neighbor spoofing, protect users from fraudulent activities, and improve user confidence in using the telecommunication system.

Table 3

Challenges in stir/shaken adoption

STIR/SHAKEN Adoption in Indonesia	Percentage	Number of Providers
Fully Implemented	17%	536
Partially Implemented	27%	817
Not Implemented	56%	1.710

Yet despite these challenges, STIR/SHAKEN has some critical advantages: it lets providers flash warnings like "possible scam" on suspicious calls, so users can make an educated choice in receiving the call. Additionally, the protocol gives way to digital trails, which allow law enforcement to track down and prosecute spoofing culprits, adding accountability. Data also shows that users in countries where STIR/SHAKEN has been adopted more broadly report fewer scam calls, underscoring the protocol's effectiveness.

C. *Mitigation Strategies*

Effectiveness studies of the approaches currently in use need to be conducted to understand the pragmatic effect and challenges accompanying the mitigation of neighbor spoofing. Each approach holds unique advantages while facing distinct limitations depending on the technological infrastructure, regulatory environment, and public engagement in place. For example, the STIR/SHAKEN protocol is the gold standard in preventing spoofing, which has dramatically reduced robocalls in countries like the United States. Still it, comes with high implementation costs and incompatibility with legacy systems. Similarly, AI-driven detection tools and call-blocking applications provide valuable supplemental defenses. However, they often rely on large datasets and user adoption, limiting their scope to end-user devices rather than system-wide enforcement. The following table compares a number of important mitigation strategies in terms of their efficacy, challenges in implementation, and examples of implementation. We can then apply this information to assess the gaps in existing measures and draft a roadmap for holistic, multi-tier protection against neighbor spoofing in telecommunication networks.

Table 4

Data for mitigation measures

Mitigation Strategy	Details	Implementation	Challenges
STIR/SHAKEN Protocol	Moderate, Not fully implemented, adoption at 17%.	Partial adoption by Indonesian telecom providers (Telkomsel, Indosat).	High cost; incompatible with legacy systems.
AI-Based Detection	Moderate, Can block 60%-70% of spam calls.	Integrated by Truecaller and Hiya in Indonesia.	Requires access to large datasets locally.
Call-Blocking Applications	Moderate, Immediate relief to 14% of active users.	Truecaller is widely used in urban areas.	Limited reach in rural regions.

V. DISCUSSIONS

Neighbor spoofing has become one of the most pressing challenges in Indonesia's telecommunication sector, where attackers exploit Caller ID manipulation to mimic local or familiar numbers. This tactic has proven highly effective, with spam calls attributed to neighbor spoofing reaching 25.8 million in January 2021, affecting millions of users. The problem is exacerbated by Indonesia's relatively weak Caller ID authentication systems and reliance on legacy infrastructure, which are ill-equipped to detect and prevent such tactics. As internet penetration reached 79.5% in 2023, attackers increasingly exploited data breaches totaling 600,000 cases 2023 to obtain personal information, making spoofed calls appear more convincing and more complex for users to detect. This has undermined public trust in telecommunication services and exposed users to financial fraud and privacy risks. The lack of systemic safeguards further compounds the issue, as existing mitigation measures, such as call-blocking applications and user reporting, are reactive and insufficient to tackle the underlying vulnerabilities.

The STIR/SHAKEN protocol offers a promising solution by authenticating Caller ID information using digital certificates, ensuring that only verified calls are routed to users. This protocol has demonstrated significant success in other countries, such as the United States, which reported a 29% reduction in robocalls shortly after its implementation. However, in Indonesia, the adoption of STIR/SHAKEN remains limited, with only 17% of telecommunication providers fully implementing it. In comparison, 56% have yet to adopt the protocol, mainly due to high costs, technical barriers, and regulatory gaps. Many smaller providers lack the financial resources to upgrade their systems, and a significant portion of Indonesia's telecommunication infrastructure remains incompatible with modern protocols like STIR/SHAKEN. Additionally, the absence of mandatory regulations requiring of robust Caller ID authentication further delays progress. Despite these challenges, opportunities exist to improve adoption. Public-private partnerships could help subsidize the costs for smaller providers, while regional collaboration with neighboring Southeast Asian countries could strengthen defenses against cross-border spoofing operations. Raising public awareness about the risks of neighbor spoofing and the benefits of STIR/SHAKEN would further encourage users and providers to prioritize secure telecommunication practices. By addressing these barriers and leveraging these opportunities, Indonesia could significantly enhance its telecommunication security and reduce the prevalence of neighbor spoofing.

VI. CONCLUSIONS

Phone spam, especially robocalling with spoofed Caller ID, has been one of the most critical problems globally, causing billions of dollars in economic losses annually. An examination of various approaches for mitigation indicates that no approach is singly up to the task of combating this problem. Each has its advantages and limitations, particularly regarding usability, deployability, and robustness against evolving threats. While STIR/SHAKEN has shown promising results as a primary mitigation technology, its full implementation faces serious challenges in countries with relatively unevenly developed telecommunication infrastructures. The core of the problem lies in the spoofing of Caller ID, which is still rampant due to incomplete deployment on the part of caller authentication mechanisms across the board.

Another recommendation from this study is to use a combination of mitigation methods to compensate for shortcomings in each technique. These mixes balance, in total, the need for usability, efficient deployment, and system resilience. For Indonesia itself, collaboration between telecommunication providers, regulators, and the public should be the starting point to speed up the implementation of solutions such as STIR/SHAKEN with stricter regulations and incentives for small providers. These measures, if taken, can reduce any threat, including neighbor spoofing, to the barest minimum and build public confidence in modern telecommunication systems.

REFERENCES

[1] Juliyana, Eva, et al. Peranan internet dalam meningkatkan citra sma swasta budi agung medan the role of the internet in improving image budi agung medan private vocational school. Feb. 2020.

[2] Murray, Teresa. Make the Ringing Stop: The FCC Is Finally Fighting Back against Robocalls. Sept. 2021.

[3] E. Norvita, A. M. Raf'ie Pratama, L. Iswari, and F. Rahma, "Blacklisting atau Aplikasi Khusus? Perspektif Pengguna Smartphone dalam Mengatasi Spam Call."

[4] Prasad, Sathvik, et al. Open Access to the Proceedings of the 29th USENIX Security Symposium Is Sponsored by USENIX. Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis. 2020.

[5] P. Dewanti, "Truecaller's Spam Call and SMS Blocking Solution for Surveillance on Social Media," 2022. [Online]. Available: www.ejournal.isha.or.id/index.php/Mekintek

[6] Kementerian Perdagangan Republik Indonesia. "PERDAGANGAN DIGITAL (E-COMMERCE) INDONESIA PERIODE 2023."

Kemendag.go.id, 2024, satudata.kemendag.go.id/ringkasan/produk/perdagangan-digital-e-commerce-indonesia-periode-2023.

[7] V. Buriachok, V. Sokolov, and T. D. Mahyar, “RESEARCH OF CALLER ID SPOOFING LAUNCH, DETECTION, AND DEFENSE,” Cybersecurity: Education, Science, Technique, vol. 3, no. 7, pp. 6–16, 2020, doi: 10.28925/2663-4023.2020.7.616.

[8] Curtin, Ashley. “Americans Report More Spam Calls in 2024 than 2023 | NationofChange.” Nationofchange.org, 10 Oct. 2024, www.nationofchange.org/2024/10/10/americans-report-more-spam-calls-in-2024-than-2023/.

[9] U. Pirg education fund, “make the ringing stop: the fcc is finally fighting back against robocalls.”

[10] Fake caller id schemes information on federal agencies’ efforts to enforce laws, educate the public, and support technical initiatives report to congressional committees united states government accountability office, 2019.

[11] I. Indriyani and P. Dewanti, “Truecaller’s Spam Call and SMS Blocking Solution for Surveillance on Social Media,” Jurnal Mekintek : Jurnal Mekanikal, Energi, Industri, Dan Teknologi, vol. 13, no. 1, pp. 19–29, Apr. 2022,

[12] A. Sharma, A. Tyagi, and M. Bhardwaj, “Analysis of techniques and attacking pattern in cyber security approach,” International journal of health sciences, pp. 13779–13798, Jun. 2022, doi: https://doi.org/10.53730/ijhs.v6ns2.8625.

[13] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, Mar. 2021, doi: https://doi.org/10.3389/fcomp.2021.563060.

[14] Federal communications commission sixth report and order in cg docket no. 17-59, fifth report and order in wc docket no. 17-97, order on reconsideration in wc docket no. 17-97, order, seventh further notice of proposed rulemaking in cg docket no. 17-59, and fifth further notice of proposed rulemaking in wc docket no. 17-97.

[15] S. Wang, “New authentication applications in the protection of caller ID and banknote - WRAP: Warwick Research Archive Portal,” Warwick.ac.uk, 2023, doi: https://wrap.warwick.ac.uk/id/eprint/181792/1/WRAP_Theses_Wang_2023.pdf.

[16] S. Pandit, M. Ahamad, D. Yang, K. Sarker, and R. Perdisci, “Combating Robocalls with Phone Virtual Assistant Mediated Interaction Combating Robocalls with Phone Virtual Assistant Mediated Interaction,” 2023.

[17] Make the ringing stop: the fcc is finally fighting back against robocalls.

[18] S. T. Zargar, J. Joshi, and D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013, doi: https://doi.org/10.1109/surv.2013.031413.00127.

[19] “STIR/SHAKEN Addressing Caller ID Spoofing 2.”

[20] H. Sahu, “SPOOFING AS A CYBER THREAT: LEGAL REMEDIES .”

[21] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, “Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review,” Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 527–555, Jul.

[22] P. Ramesh and D. Lalitha. Bhaskari, “A Comprehensive Analysis of Spoofing,” International Journal of Advanced Computer Science and Applications, vol. 1, no. 6, 2010.

[23] I. M. Tas and S. Baktir, “Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks,” IEEE Access, vol. 12, pp. 60123–60137, 2024, doi: https://doi.org/10.1109/access.2024.3393487.

[24] R. Ranjan, M. Vatsa, and R. Singh, “Uncovering the Deceptions: An Analysis on Audio Spoofing Detection and Future Prospects,” Jul. 2023.

[25] A.-D. Hofnăr, T. Bakos, and G. Sebestyen-Pal, “Protecting Against Caller ID Spoofing Attacks Using In-band Signaling,” 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 263–268, Oct. 2023, doi: https://doi.org/10.1109/iccp60212.2023.10398672.

[26] J. McEachern and E. Burger, “How to shut down robocallers: The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole,” IEEE Spectrum, vol. 56, no. 12, pp. 46–52, Dec. 2019, doi: https://doi.org/10.1109/mspec.2019.8913833.

[27] M. A. Azad, M. Alazab, F. Riaz, J. Arshad, and T. Abullah, “Socioscope: I know who you are, a robo, human caller or service number,” Future Generation Computer Systems, vol. 105, pp. 297–307, Apr. 2020, doi: https://doi.org/10.1016/j.future.2019.11.007.

[28] C.-Y. Yu, C. K. Chang, and W. Zhang, “An Edge Computing Based Situation Enabled Crowdsourcing Blacklisting System for Efficient Identification of Scammer Phone Numbers,” 2020 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 776–781, Dec. 2020, doi: https://doi.org/10.1109/csci51800.2020.00146.

[29] “CRIMINAL LIABILITY FOR CLI SPOOFING,” vol. 3, no. 2, Dec. 2023, doi: https://doi.org/10.57599/gisoj.2023.3.2.37.

[30] S. Pandit, J. Liu, R. Perdisci, and M. Ahamad, “Applying Deep Learning to Combat Mass Robocalls,” 2021 IEEE Security and Privacy Workshops (SPW), pp. 63–70, May 2021, doi: https://doi.org/10.1109/spw53761.2021.00018.