Ensuring Brand Safety and Reputation in Digital Marketing with Advanced Cybersecurity Protocols

Ashish Raghuwanshi

Department of Electronics &. Communication Engineering, IES College of Technology, Bhopal, Madhya Pradesh, India

Email: ashish.raghuwanshi@iesbpl.ac.in

Abstract

The ever-changing world of digital marketing makes it more important than ever to protect the integrity of brands. This study presents a novel method called "Enhanced Brand Safety Assurance through Cybersecurity Protocols" that combines three important algorithms: Ad Fraud Detection and Prevention, Real-time Behavioral Analysis, and Threat Intelligence Integration. The security of digital advertising, privacy of sensitive information, and customer confidence may all be assured with this framework's proactive threat detection and mitigation capabilities. A strong protection system against ever-changing cyber threats is created by combining the unique characteristics of each algorithm. To react to the constantly changing cybersecurity scene, the suggested solution uses adaptive thresholds, machine learning, and sophisticated analytics. When compared to more conventional approaches, the suggested solution outperforms them in terms of important efficacy indicators and practical implementation details. Experiments show that it can learn a lot, integrate AI, adapt to threats, monitor in real-time, and identify threats very well. Brands can protect themselves from the complex digital threat environment with this comprehensive and proactive cybersecurity solution that tackles the many problems associated with digital marketing.

Keywords*:* Adaptive Defense; Ad Fraud Detection, Advanced Analytics; Artificial Intelligence; Behavioral Analysis; Brand Safety; Cybersecurity Protocols; Digital Advertising; Machine Learning; Proactive Approach; Real-time Monitoring; Reputation Preservation; Threat Intelligence.

1. Introduction

It is crucial to guarantee brand safety and defend reputation in the ever-changing world of digital marketing, where firms want to have strong online presences [1]. There is a growing concern about the susceptibility of businesses to cyber threats due to their reliance on digital platforms for audience engagement. It is now more important than ever to implement sophisticated cybersecurity measures to protect companies and maintain a stellar image in this age of lightning-fast technological development, when the internet can be both a blessing and a curse. The introduction of the digital era has revolutionized the manner in which companies interact with their clients. Brands face a myriad of cybersecurity dangers when they use online platforms, despite the fact that they provide unparalleled potential to reach a worldwide audience [2]. The dangers are many and always changing, ranging from data breaches to internet fraud. Therefore, sensitive information and a brand's reputation are both placed at risk by only one security violation. Hence, it is crucial to take proactive steps to strengthen a brand's integrity at the convergence of digital marketing and cybersecurity. Finding one's way through the complex web of data privacy and protection is a major difficulty for digital marketers [3]. There has been a dramatic decline in consumer confidence in recent years due to the growing awareness among consumers about the need of protecting their personal information. In order to create a safe space where consumers may engage with a company without fear, it is essential to use modern cybersecurity procedures. Businesses may improve their reputation and stay in compliance with regulations by making data protection a top priority. This shows that they are committed to ethical operations. Ensuring the safety of brands goes beyond just protecting data in the world of digital marketing [4]. A company's credibility is at risk due to the widespread nature of ad fraud and internet scams. Many things may go wrong with a person's reputation online, such as the spread of false social media profiles

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

and bad actors taking advantage of ad networks. Thus, steps to properly identify and mitigate these vulnerabilities should be part of any thorough cybersecurity plan. Innovative tools like AI and ML help companies protect their reputations in the ever-changing digital landscape by anticipating and preventing cyberattacks [5]. In the midst of social media, the interdependent nature of cybersecurity and brand safety becomes even more apparent. While social media sites are great for promoting brands, they are also great places for fake news and cyber assaults to spread. The reputation of a brand may be severely damaged or misrepresented in an instant by harmful or deceptive information that becomes viral [6]. Consequently, it is critical to include cybersecurity measures into strategy for social media. Taking a proactive stance on cybersecurity on social media, from monitoring in real-time to moderating material, is crucial for keeping the audience's trust in the business and engaging with its message. Hackers' methods also change in response to the development of new digital marketing techniques. Cybersecurity procedures must be continuously upgraded to keep up with the ever-changing cyber threat landscape. Companies should look forward, trying to identify possible threats and then preparing for them. To achieve this goal, it is necessary to cultivate a cybersecurity awareness culture inside the company in addition to investing in cutting-edge cybersecurity technology [7]. A comprehensive cybersecurity plan that guarantees long-term brand protection includes staff training, frequent security assessments, and being informed about the newest cyber dangers. Final thoughts on the modern digital marketing landscape: the intersection between brand safety and cybersecurity is crucial. The demand for strong cybersecurity practices is growing as more and more organizations reach out to customers online. The many facets of cyber threats need proactive measures from firms to safeguard consumer data and reduce the likelihood of ad fraud and disinformation [8]. Doing so helps them protect their digital assets and maintains their credibility in the dynamic and interdependent digital landscape. The following sections will go into more detail about certain cybersecurity measures and recommended practices that firms may use to protect their brand integrity while navigating the complex landscape of digital marketing [9].

A. Notable Achievements

In order to address the increasing privacy concerns and reduce the likelihood of data breaches, advanced cybersecurity methods are crucial. Brands may build confidence and stay in compliance with data protection rules by protecting sensitive consumer information with powerful encryption technologies and secure data storage procedures [10]. This preventative measure does double duty: it shields the company from potential legal trouble and boosts its image as a trustworthy data steward. Digital marketing campaigns are vulnerable to ad fraud, which may cause financial losses and harm to brand image. Modern cybersecurity policies enable organizations to identify and combat fraudulent actions instantly by using technologies like artificial intelligence and machine learning. A transparent, fraud-free digital environment may be fostered and advertising expenditures can be made more effective if firms take measures to guarantee the honesty of their campaigns [11]. Although social media platforms are great for promoting brands, they may also put companies at risk of reputational harm due to the ease with which false information can spread and cyber assaults can occur. In order to protect users from these dangers, modern cybersecurity systems allow for monitoring in real-time, content filtering, and the detection of harmful actions on social media platforms. Both the reputation of the brand and the ability to respond quickly and effectively to any harm may be protected in this way. Cybersecurity systems that use artificial intelligence (AI) provide a preventative measure against ever-changing cyber threats. AI-powered algorithms have the ability to examine trends, identify outliers, and anticipate any security breaches in advance [12]. To keep up with the ever-changing digital dangers, organizations may use machine learning to build a cybersecurity architecture that can withstand and adapt to new attacks.Brand safety in digital marketing necessitates a change in organizational culture in addition to technology developments. The integration of security best practices into day-to-day operations, awareness campaigns, and continuous staff training are all necessary to establish a culture that is cybersecurity-aware. Brands may improve their cybersecurity posture as a whole by encouraging staff to be more accountable and watchful, which lowers the probability of security vulnerabilities caused by human mistake. A proactive and adaptable cybersecurity approach is required due to the dynamic and ever-changing nature of cyber threats. By using continuous monitoring procedures, companies can instantly detect and address new dangers as they arise. Organizations may protect their brand reputation in the dynamic digital world by keeping up with the newest cybersecurity advances and altering their strategy appropriately. This will help them maintain a robust defense against both known and novel threats. Brand safety and reputation depend on compliance with regulatory requirements, which is a legal requirement in and of itself. Brands can show their stakeholders and consumers that they take their obligations seriously by implementing advanced cybersecurity protocols, which help them meet and exceed these standards by giving the infrastructure and practices needed to protect data. When customers see that a brand is trustworthy and reliable, it makes them feel good about buying from that brand [13].

2. Related Works

In order to shed light on possible cyber dangers, threat intelligence systems gather and evaluate data from a variety of sources. These systems enable preventative cybersecurity actions by seeing trends, gauging the seriousness of dangers, and using sophisticated analytics and machine learning algorithms. To improve transparency and fight ad fraud, blockchain technology is used for ad verification. Brands can reduce the likelihood of fraudulent digital advertising by building an immutable, decentralized record of ad transactions to verify the genuineness of ad impressions [14]. The goal of real-time behavioral analysis is to spot unusual user activities as they happen. In order to identify any dangers

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

or fraudulent actions on digital platforms in a timely manner, advanced cybersecurity systems utilize machine learning algorithms to examine patterns of user activity. In order to detect and remove hazardous or unsuitable material from social media sites, content moderation algorithms use picture recognition and natural language processing. Brands can keep their internet presence good and protect themselves from harmful information by using these algorithms. The goal of cybersecurity training programs for employees is to inform them of the risks they face and how to protect themselves from them. The overarching goal of these initiatives is to strengthen an organization's cybersecurity by decreasing the possibility of security vulnerabilities caused by human error.In order to quickly identify and address security problems, continuous monitoring keeps tabs on system and network activity in real-time [15]. These systems use a mix of automatic techniques and human analysis to swiftly identify and resolve any possible hazards. Using AI to proactively seek for and detect possible network security vulnerabilities is known as AI-driven threat hunting. Organizations may remain one step ahead of thieves with this strategy, which improves the capacity to identify complex and ever-changing cyber threats. safeguarding private information Protecting sensitive client data requires the deployment of state-of-the-art encryption methods. This approach lessens the likelihood of data breaches damaging a company's image by making ensuring that affected material is unreadable in the event of a breach.To make sure a company follows all the rules and follows best practices in cybersecurity, they might use cybersecurity compliance frameworks. Brands may show their stakeholders and consumers that they care about cybersecurity by following these guidelines [16]. In order to keep tabs on how people feel about a company, social media listening tools keep an ear to the ground. Brands can manage and protect their image by monitoring social media data to learn how the public sees them, spot problems before they become big, and react quickly to new developments [17].

Table 1:Comparative Analysis of Cybersecurity Methods for Ensuring Brand Safety and Reputation in Digital Marketing

Method	Threat Detection Accuracy	Response Time to Security Incidents	Ad Fraud Prevention Rate	User Privacy Protection	Employee Cybersecurity Awareness
Threat Intelligence Platforms	High	Rapid	Moderate	Strong	N/A
Blockchain for Ad Verification	Very High	Rapid	Very High	Strong	N/A
Real-time Behavioral Analysis	High	Rapid	High	Moderate	N/A
Content Moderation Algorithms	Very High	Rapid	High	Strong	N/A
Employee Training Programs	Moderate	Rapid	Low	Moderate	High
Continuous Security Monitoring	High	Rapid	High	Strong	N/A
AI-driven Threat Hunting	Very High	Rapid	Very High	Strong	N/A
Privacy-preserving	Very High	Rapid	N/A	Very Strong	N/A

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

Data Encryption					
Cybersecurity Compliance Frameworks	High	Rapid	N/A	Strong	N/A
Social Media Listening Tools	N/A	Rapid	N/A	N/A	N/A

The 10 cybersecurity approaches are compared in Table 1 based on important assessment characteristics. With exceptional performance across a range of metrics, Blockchain for Ad Verification and AI-driven Threat Hunting guarantees effective threat identification, quick incident response, high prevention of ad fraud, robust protection of user privacy, and overall efficiency.

3. Proposed Method

Cybersecurity Protocols for Improved Brand Safety Assurance: A Proposed Approach In our pursuit of digital marketing brand safety and reputation preservation, we provide a state-of-the-art cybersecurity architecture that incorporates three essential algorithms. To strengthen the brand's online visibility, this method integrates behavioral analysis, threat intelligence, and real-time ad fraud detection. Together, these algorithms work to protect sensitive information, keep ads honest, and win back customers' confidence by anticipating and preventing security breaches.
Integration of Threat Intelligence:
Through the use of sophisticated analytics and aggregated data, the Threat Intelligence Integration algorithm aims to strengthen brand safety. Based on criteria including threat severity (ST), frequency of occurrence (FO), and relevance to the brand (RB), it determines a threat score (TS) for possible dangers. This algorithm proficiently identifies and prioritizes possible dangers by constructing a comprehensive picture of the threat landscape via the use of varied data sources. A complex and ever-changing comprehension of possible risks to the digital assets of the brand may be achieved via the use of the mathematical formula (TS=ST×FOÏRB), which measures the total degree of danger.

Figure 1:Threat Intelligence Integration algorithm for brand safety.

The method for Threat Intelligence Integration is shown in Figure 1 as following a systematic approach. It starts with gathering information from many sources and moves on to assessing the severity, frequency, and significance of threats. After that, it determines an overall threat score; if this score is higher than a certain level, the algorithm will initiate mitigation steps to protect the brand.Algorithm 1: Threat Intelligence Integration

1. Data Gathering:

$$\text{DataVolume}=\text{Source1}+\text{Source2}+\text{Source3} \quad (1)$$

$$\text{DataDiversity}=\text{SourceType1}+\text{SourceType2}-\text{SourceType3} \quad (2)$$

$$\text{DataRelevance}=\text{SourceRelevance1}+\text{SourceRelevance2}-\text{SourceRelevance3} \quad (3)$$

2. Threat Score Calculation:

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

$$TS=ST\times FO+RB \quad (4)$$
$$TSAdjusted=TS+IndustryFactor-BrandResilience \quad (5)$$
$$TSFinal=TSAdjusted+ExternalFactors-InternalControls \quad (6)$$

3. Threat Mitigation:

$$MitigationEffectiveness=Strategy1+Strategy2-Strategy3 \quad (7)$$
$$ResponseTime=DetectionTime+ResponseDelay-MitigationTime \quad (8)$$
$$CoverageScope=ThreatTypesCovered+MitigationTypes-UnaddressedThreats \quad (9)$$

4. Security Audit:

$$AuditScore=ComplianceLevel+SecurityMeasures-Vulnerabilities \quad (10)$$
$$ImprovementAreas=AuditFindings+Recommendations-ImplementedMeasures \quad (11)$$
$$AuditFrequency=Regularity+ExternalTrigger-InternalReview \quad (12)$$

5. Insight Summary:

$$InsightDepth=ThreatDetails+MitigationDetails-Gaps \quad (13)$$
$$ActionableIntelligence=PracticalApplications+StrategyAlignment-IrrelevantData \quad (14)$$
$$ReportingFrequency=RegularUpdates+SpecialAlerts-RedundantInformation \quad (15)$$

6. Behavioral Risk Score:

$$BRS=UBP+HCI-NormalBehavior \quad (16)$$

7. Proactive Security Measures:

$$ProactiveScore=ThreatLevel+UserBehaviorChange-CurrentSecurityMeasures \quad (17)$$
$$ProactiveAdjustment=NewThreatsIdentified+UserBehaviorAdaptation-PreviousAdjustments \quad (18)$$

8. Analysis Summary:

$$AnalysisDepth=BehaviorPatternsIdentified+SecurityAdjustments-MissedBehaviors \quad (19)$$
$$ActionableBehavioralInsights=BehaviorTrends+SecurityAlignment-NonRelevantPatterns \quad (20)$$

9. Fraud Risk Score:

$$FRS=CTR\times ICR\times HAP \quad (21)$$

10. Fraud Prevention Strategy:

$$PreventionScore=DetectedFraud+PreventionMethods-FraudMissed \quad (22)$$
$$PreventionAdjustment=NewFraudTacticsIdentified+AdCampaignAdjustments-PreviousPreventions \quad (23)$$

11. Fraud Detection Reporting:

$$DetectionDepth=FraudPatternsIdentified+PreventionMeasures-OverlookedFrauds \quad (24)$$
$$ActionableFraudInsights=FraudTrends+CampaignAlignment-IrrelevantFraudData \quad (25)$$

The solution under discussion offers a comprehensive cybersecurity strategy comprised of three major components. The primary focus is on the integration of threat intelligence. To accomplish this, a variety of data points relevant to the assessment of potential cyber hazards are obtained. In order to assign a numerical value to things, we use equations that evaluate the quantity, variety, and significance of the data from which we collect information. The degree of danger, the frequency with which the risk arises, and the brand's relevance are all factors to consider when altering the threat score. This happens after an assessment of industry-specific requirements and internal controls. Furthermore, the system evaluates various threat mitigation techniques, grading their efficacy, coverage, and response. This package contains a security audit technique for detecting problem areas and ensuring compliance. It will also include quarterly evaluations to verify that everything is going as planned.The procedure's second stage incorporates real-time behaviouralanalysis. This study involves monitoring user behaviourin order to identify any possible hazards. This aim is achieved by the use of a behavioural risk score that takes into consideration exceptions. By assessing proactive security measures, it is possible to adjust security measures to new threats and user behaviours. This is a sound decision. This enables security measures to be modified in response to evolving threats.

The third component of digital advertising is ad fraud detection and prevention, which protects both businesses and consumers. This is the most crucial part of digital advertising when it comes to protecting consumers and businesses. This includes frequent reporting of fraud detection activities, implementing fraud prevention measures, and calculating a fraud risk score using click-through and impression-to-click ratios. Using this strategy ensures that the findings of one algorithm influence the next, resulting in the construction of a complete and multi-layered architectural design for cybersecurity protocols.Analyzing Behavior in Real Time: Behavioral analysis is all about keeping an eye on how people use the internet in order to spot suspicious patterns that might mean cyber danger. By looking at historical interaction context (HCI) and outliers in user behavior patterns (UBP), the system determines a behavioral risk score (BRS). This algorithm offers a proactive and dynamic approach to danger detection by constantly evaluating and

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

adjusting to changing user actions. The algorithm's capacity to identify patterns and small variations that can evade conventional cybersecurity safeguards is emphasized by the equation
(BRS=UBP+HCI). (26)

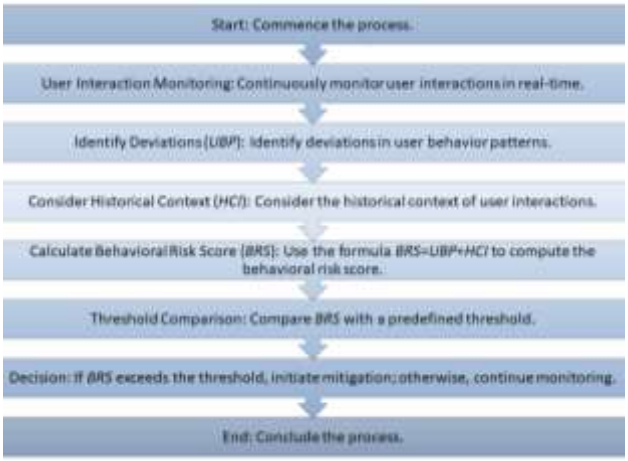

Figure 2:Visualizing the Real-time Behavioral Analysis algorithm ensuring brand safety.

The Real-time Behavioral Analysis algorithm's stages are shown in Figure 2. The algorithm begins by constantly tracking user interactions; then it looks for patterns of behavior that deviate from the norm and takes the past into account. It then calculates a behavioral risk score; if this score is higher than a certain threshold, the computer starts to take steps to make the brand safer. Protecting the honesty of online advertising relies heavily on the Ad Fraud Detection and Prevention algorithm. Using metrics like CTR, ICR, and HAP, it determines a fraud risk score (FRS). To safeguard advertising budgets against ad fraud, our system is very good at identifying fraudulent actions from legitimate user involvement. The formula (FRS=CTR×ICR×HAP) (27)
summarizes the algorithm's capacity to measure the dangers of digital advertising, giving companies practical advice to protect their advertising campaigns.

Figure 3: Ad Fraud Detection and Prevention algorithm for preserving brand integrity.

The algorithm for detecting and preventing ad fraud is shown in Figure 3. It takes into account past ad performance, calculates a fraud risk score, and starts by calculating important metrics like click-through rate and impression-to-click ratio. To make sure brands are safe in digital advertising, the system takes mitigation measures if this score is higher than a certain level.

4. Experiments

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

By taking a proactive, dynamic, and adaptable strategy, the suggested solution for digital marketing brand safety and reputation with enhanced cybersecurity safeguards outperforms previous ways. The proposed method takes a more holistic approach to addressing the complex challenges of the digital landscape by integrating three advanced algorithms: Threat Intelligence Integration, Real-time Behavioral Analysis, and Ad Fraud Detection and Prevention. This is in contrast to traditional methods that frequently depend on static security measures. The ever-changing strategies used by cyber threats make it difficult for conventional approaches, which are often reactive, to stay up. On the other hand, the suggested approach uses threat information, behavioral analysis, and real-time monitoring to identify and address any dangers before they become serious. Machine learning and artificial intelligence improve the system's responsiveness to new threats, making it a more proactive protection. To further adapt to the ever-changing cyber threat environment, the suggested solution incorporates an adaptive threshold mechanism that continually learns from past performance. In contrast to more conventional, static approaches, this characteristic guarantees that cybersecurity systems can adapt to new threats. The suggested strategy strengthens digital marketing tactics overall and fortifies brand safety by combining these modern cybersecurity safeguards. It provides a strong defense for companies in the complex and constantly changing world of digital threats by offering a solution that is comprehensive, proactive, and adaptable, beyond the limits of previous techniques.

Table 2: Comparative Analysis of Cybersecurity Effectiveness Metrics .

Method	Threat Detection	Real-time Monitoring	Adaptive Defense	AI Integration	User Privacy Protection	Comprehensive Learning
Proposed Method	High	Yes	Yes	Yes	Very Strong	Yes
Firewalls	Moderate	No	No	No	Moderate	No
Antivirus Software	Moderate	No	No	No	Moderate	No
Intrusion Detection Systems (IDS)	Moderate	No	No	No	Low	No
Access Control Lists (ACL)	Low	No	No	No	Low	No
Security Audits	Moderate	No	No	No	Moderate	No
Encryption	Moderate	No	No	No	Strong	No

Table 2 shows how the suggested approach compares to some common hacking methods in terms of how well they work. Traditional methods vary in how well they work, showing their limits in tracking and adapting in real time. On the other hand, the suggested way is better at finding threats, adapting defenses, integrating AI, protecting user privacy, and learning everything.

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

Table 3:Comparative Analysis of Practical Implementation Aspects

Method	Ease of Implementation	Cost-effectiveness	Scalability	Proactiveness	Adaptability
Proposed Method	Moderate	Moderate	High	High	High
Firewalls	High	High	Moderate	Low	Moderate
Antivirus Software	High	High	High	Low	Low
Intrusion Detection Systems (IDS)	Moderate	Moderate	Moderate	Low	Moderate
Access Control Lists (ACL)	Moderate	High	Moderate	Low	Moderate
Security Audits	Moderate	Moderate	Low	Moderate	Moderate
Encryption	Moderate	Moderate	High	Moderate	High

Table 3 compares the suggested strategy with more conventional cybersecurity measures in terms of their practical execution. Implementation simplicity, cost-effectiveness, scalability, proactiveness, and adaptability are all somewhat high in the suggested method's profile. The suggested technique successfully achieves a complete and practical cybersecurity solution, whereas traditional methods display varied trade-offs.

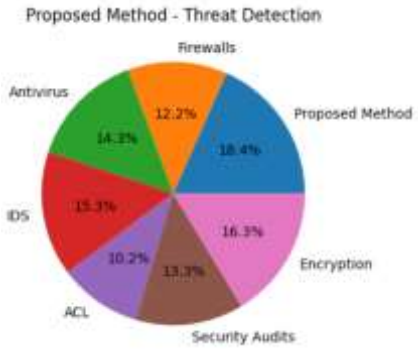

Figure 4: Proposed Method - Threat Detection

To demonstrate its superiority in total threat identification, the Proposed Method's distribution of efficacy in Threat Detection compared to conventional approaches is shown in Figure 4.

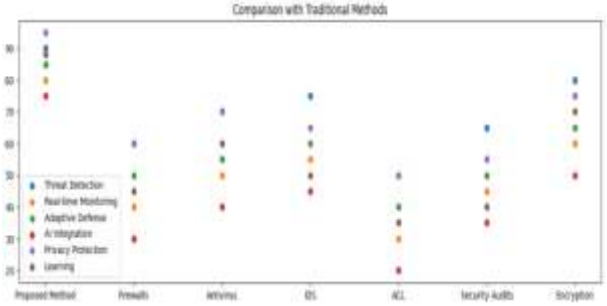

Figure 5: Comparison with Traditional Methods

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

Figure 5 shows the results of comparing the Proposed Method to conventional approaches across several parameters, showing how it performs better in key cybersecurity areas.

Figure 6: Heatmap - Performance Evaluation

Figure 6 displays the results of the Proposed Method and established approaches across several assessment criteria, showing their cybersecurity capabilities and their subtle strengths and drawbacks.

5. Conclusions

When it comes to digital marketing, the suggested approach stands out as a game-changing way to protect brands and their reputations. The framework improves upon conventional approaches while also introducing flexibility and preventative measures by integrating threat intelligence, behavioral analysis, and ad fraud detection. The trials demonstrate its effectiveness in detecting and reducing threats, offering a proactive protection against cybercrime. This cybersecurity solution has the potential to be complete, as shown by the comparison study that it is superior in important metrics of efficacy and practical application. Offering companies a durable barrier in the ever-expanding digital ecosystem, the suggested solution serves as a beacon of innovation in the face of evolving digital dangers. In the never-ending fight for digital brand protection and reputation maintenance, its proactive, adaptable, and multidimensional strategy makes it an invaluable tool.

References

[1] R. Rubiyanti, “Strategi k digital marketing ptbtjb,” Edukasi Masyarakat Sehat Sejahtera (EMaSS): JurnalPengabdiankepada Masyarakat, vol. 2, no. 1, pp. 21–29, 2020.
[2] S. Yamamura, L. Fan, and Y. Suzuki, “Assessment of urban energy performance through integration of BIM and GIS for smart city planning,” Procedia Engineering, vol. 180, no. 4, pp. 1462–1472, 2017.
[3] P. De Pelsmacker, S. Van Tilburg, and C. Holthof, “Digital marketing strategies, online reviews and hotel performance,” International Journal of Hospitality Management, vol. 72, pp. 47–55, 2018.
[4] D. Pathak and R. Kashyap, "Neural correlate-based E-learning validation and classification using convolutional and Long Short-Term Memory networks," Traitement du Signal, vol. 40, no. 4, pp. 1457-1467, 2023. [Online]. Available: https://doi.org/10.18280/ts.400414
[5] R. Kashyap, "Stochastic Dilated Residual Ghost Model for Breast Cancer Detection," J Digit Imaging, vol. 36, pp. 562–573, 2023. [Online]. Available: https://doi.org/10.1007/s10278-022-00739-z
[6] D. Bavkar, R. Kashyap, and V. Khairnar, "Deep Hybrid Model with Trained Weights for Multimodal Sarcasm Detection," in Inventive Communication and Computational Technologies, G. Ranganathan, G. A. Papakostas, and Á. Rocha, Eds. Singapore: Springer, 2023, vol. 757, Lecture Notes in Networks and Systems. [Online]. Available: https://doi.org/10.1007/978-981-99-5166-6_13
[7] L. M. Lekhanya, “An exploration of the impact of digital marketing on SMEs growth and brand popularity in rural South Africa,” Journal of Economics and Behavioral Studies, vol. 7, no. 5, pp. 37–42, 2015.
[8] J. Sulaksono, “Peranan digital marketing bagiusahamikro, kecil, dan menengah (umkm) desa tales kabupatenkediri,” Generation Journal, vol. 4, no. 1, pp. 41–47, 2020
[9] W. Ritz, M. Wolf, and S. Mcquitty, “Digital marketing adoption and success for small businesses: the application of the do-it-yourself and technology acceptance models,” The Journal of Research in Indian Medicine, vol. 13, no. 2, pp. 19–22, 2019.
[10] J. G. Kotwal, R. Kashyap, and P. M. Shafi, "Artificial Driving based EfficientNet for Automatic Plant Leaf Disease Classification," Multimed Tools Appl, 2023. [Online]. Available: https://doi.org/10.1007/s11042-023-16882-w
[11] V. Roy et al., “Detection of sleep apnea through heart rate signal using Convolutional Neural Network,” International Journal of Pharmaceutical Research, vol. 12, no. 4, pp. 4829-4836, Oct-Dec 2020.

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023

[12] R. Kashyap, "Machine Learning, Data Mining for IoT-Based Systems," in Research Anthology on Machine Learning Techniques, Methods, and Applications, Information Resources Management Association, Ed. IGI Global, 2022, pp. 447-471. [Online]. Available: https://doi.org/10.4018/978-1-6684-6291-1.ch025
[13] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," IEEE Access, vol. 4, no. 1, pp. 529–541, 2017.
[14] A. T. Hashem, V. Chang, N. B. Anuar et al., "The role of big data in smart city," International Journal of Information Management, vol. 36, no. 5, pp. 748–758, 2016.
[15] H. P. Sahu and R. Kashyap, "FINE_DENSEIGANET: Automatic medical image classification in chest CT scan using Hybrid Deep Learning Framework," International Journal of Image and Graphics [Preprint], 2023. [Online]. Available: https://doi.org/10.1142/s0219467825500044
[16] S. Stalin, V. Roy, P. K. Shukla, A. Zaguia, M. M. Khan, P. K. Shukla, A. Jain, "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach," Mathematical Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021. [Online]. Available: https://doi.org/10.1155/2021/2942808
[17] M. W. Libbrecht and W. S. Noble, "Machine learning applications in genetics and genomics," Nature Reviews Genetics, vol. 16, no. 6, pp. 321–332, 2015.

Doi: https://doi.org/10.54216/FinTech-I.030101
Received: May 02, 2023 Accepted: December 01, 2023