Computer Fraud and Security
ISSN (online): 1873-7056

DNS over HTTPS (DoH) in Gaming: Balancing Privacy and Threat Visibility

Sanat Talwar
Dept. of Security
Electronic Arts, Inc.
Austin, Texas sanattalwar1994@gmail.com

Abstract—

DNS over HTTPS (DoH) has emerged as a revolutionary protocol for enhancing user privacy by encrypting DNS queries, thus protecting them from eavesdropping, manipulation, and surveillance. While this technological advancement addresses increasing concerns regarding data privacy, its implementation within gaming ecosystems presents considerable cybersecurity challenges. Gaming platforms, which heavily depend on DNS for essential operations such as matchmaking, geolocation, and content delivery, now confront a critical issue: balancing robust threat visibility with the need to uphold player privacy. Traditional security tools, which rely on monitoring plaintext DNS traffic, become ineffective in DoH-integrated environments, resulting in blind spots that can facilitate malicious activities like phishing, DNS tunneling, and distributed denial-of-service (DDoS) attacks. This paper examines the implications of DoH within the gaming sector, emphasizing the trade-offs between privacy and threat visibility. We propose a hybrid framework that utilizes encrypted DNS for privacy enhancement while enabling threat detection through on-device monitoring, behavioral analysis, and machine learning techniques. By evaluating DNS query patterns and incorporating real-time threat intelligence, our framework effectively identifies and mitigates risks without infringing on player privacy. Case studies from multiplayer gaming platforms illustrate the effectiveness of our approach, demonstrating its capacity to detect and neutralize DNS-based attacks with minimal latency and high accuracy. Our findings highlight the necessity for adaptive security measures in gaming infrastructures that strike a balance between the critical goals of privacy and protection. This research advances the existing knowledge on DNS security in gaming by offering practical solutions for an industry increasingly reliant on encrypted protocols. By tackling the challenges associated with DoH adoption, this paper provides a strategic framework for gaming platforms to enhance cybersecurity while respecting player privacy.

Index Terms— subdomain takeover, cloud-native security, gaming platform vulnerabilities, DNS misconfigurations, real-time security monitoring, automated subdomain detection, DNS enumeration, certificate transparency monitoring, machine learning in cybersecurity, active reconnaissance, expired cloud services, gaming cybersecurity threats, subdomain hijacking, cloud infrastructure security

I. INTRODUCTION

The Domain Name System (DNS) represents a fundamental component of the internet, functioning as the essential mechanism for converting human-friendly domain names into machine-readable IP addresses. In the realm of online gaming,

DNS is crucial for facilitating key functions such as matchmaking, server selection based on geolocation, and content delivery. For example, when a player enters a multiplayer game, DNS guarantees their device connects to the most suitable server based on latency and geographic proximity, thereby enhancing the overall gaming experience. Nevertheless, despite its significance, DNS is inherently susceptible to numerous cyber threats, including cache poisoning, distributed denial of-service (DDoS) attacks, and subdomain hijacking[2]. These vulnerabilities are particularly alarming in gaming contexts, where low-latency performance and real-time interactions are vital to sustaining player satisfaction and competitive fairness[6]. In recent years, the implementation of DNS over HTTPS (DoH) has represented a substantial advancement in internet privacy. By encrypting DNS queries through HTTPS, DoH thwarts eavesdropping, manipulation, and surveillance by malicious entities, internet service providers (ISPs), and advertisers. This protocol has been widely embraced across various sectors, including gaming, where safeguarding player privacy is increasingly prioritized. For gaming platforms, DoH provides a mechanism to shield sensitive player data, including geolocation information and browsing habits, from exploitation by third parties. However, while DoH addresses privacy concerns, its adoption presents new cybersecurity challenges[8]. Traditional monitoring tools, which depend on analyzing plaintext DNS traffic, become ineffective in DoHenabled settings. This creates a significant blind spot for

malicious activities such as phishing, DNS tunneling, and DDoS attacks, all of which can disrupt gameplay, compromise user data, and tarnish the reputations of gaming platforms. The gaming industry currently faces a critical juncture, navigating the dual responsibilities of safeguarding player privacy and ensuring robust cybersecurity. On one side, players demand enhanced privacy protections, particularly in light of high-profile data breaches and escalating regulatory scrutiny. Conversely, gaming platforms must secure their infrastructures against the evolving threats posed by DNS vulnerabilities[9]. The lack of visibility into encrypted DNS traffic complicates this balancing act, as security teams can no longer depend on traditional methods for threat detection and mitigation. This dilemma is further intensified by the unique characteristics of gaming environments, which prioritize low-latency performance and real-time interactions. Consequently, any security solution must be designed to be lightweight, efficient, and minimally intrusive to avoid compromising the player's experience. This paper aims to tackle these challenges by proposing a framework that harmonizes privacy and security in DoH-enabled gaming environments. Our methodology employs on-device monitoring, behavioral analysis, and machine learning to facilitate threat detection without jeopardizing player privacy[7]. By examining DNS query patterns and incorporating realtime threat intelligence, the framework identifies and addresses risks such as phishing, DNS tunneling, and DDoS attacks. Case studies from multiplayer gaming platforms illustrate the effectiveness of this approach, demonstrating its capability to detect and neutralize threats with negligible latency and high accuracy[5]. The main objectives of this paper are threefold. First, we investigate the implications of DoH adoption within gaming ecosystems, emphasizing its privacy benefits and the challenges it presents for threat visibility. Second, we analyze the evolving threat landscape in DoH-enabled gaming environments, pinpointing emerging risks such as DNS tunneling and phishing[1]. Third, we propose a hybrid framework that merges encrypted DNS for privacy with advanced threat detection techniques, offering a pragmatic solution for gaming platforms as they navigate the complexities associated with DoH adoption. This research contributes significantly to the field of DNS security in gaming. First, it offers an exhaustive analysis of the trade-offs between privacy and threat visibility in DoHenabled environments, providing essential insights for gaming platforms and cybersecurity professionals. Second, it introduces an innovative hybrid framework that facilitates threat detection without compromising player privacy, addressing a crucial gap in current security protocols. Third, it presents practical case studies and experimental findings, showcasing the real-world applicability of the proposed framework. Finally, it provides recommendations for gaming platforms pursuing DoH adoption, including strategies for compliance, scalability, and performance optimization[4]. The remainder of this paper is organized as follows:. Section 2 offers an overview of DNS over HTTPS (DoH) and its ramifications for gaming. Section 3 delineates the threat landscape within DoH-enabled gaming ecosystems, emphasizing emerging risks and attack vectors. Section 4 outlines the proposed hybrid framework for reconciling privacy and threat visibility, detailing its components and implementation workflow. Section 5 describes the experimental evaluation of the framework, including methodology, results, and discussion. Lastly, Section 6 concludes the paper and sets forth directions for future research[13].

II. OVERVIEW OF DNS OVER HTTPS (DOH) AND ITS RAMIFICATIONS FOR GAMING

DNS over HTTPS (DoH) is an advanced protocol crafted to significantly improve the privacy and security of DNS queries by encapsulating them within HTTPS traffic. In contrast to conventional DNS, where queries are transmitted in plaintext and are susceptible to interception or manipulation, DoH encrypts these queries to avert eavesdropping and tampering.

This encryption leverages the extensive HTTPS infrastructure, thereby ensuring that DNS requests are secure and indistinguishable from standard web traffic. Consequently, DoH effectively mitigates risks linked to DNS spoofing, cache poisoning, and other forms of DNS-related attacks, ultimately enhancing the safety of the user's browsing experience[16]. Within the realm of online gaming, the implementation of DoH presents a dual-edged impact. On the positive side, gaming platforms benefit substantially from the enhanced privacy that DoH provides. With encrypted DNS queries, sensitive player information—such as geolocation and browsing habits—remains confidential, protecting it from potential exploitation by malicious actors or intrusive service providers. This heightened level of privacy is especially crucial in an age characterized by frequent data breaches and unauthorized surveillance, alongside increasingly stringent regulatory requirements. The protective layer offered by DoH fosters player trust and ensures that gaming environments adhere to evolving data protection standards[12]. Conversely, the integration of DoH into gaming ecosystems also introduces notable cybersecurity challenges. Traditional

network security tools depend heavily on the inspection of DNS traffic in plaintext to identify anomalies, malicious patterns, or indicators of compromise. The shift to encrypted DNS renders these conventional approaches largely ineffective, creating blind spots that adversaries may exploit. This diminished visibility can impede the detection of sophisticated threats such as DNS tunneling—where attackers conceal malicious activities within encrypted traffic—or coordinated DDoS attacks aimed at disrupting gaming services. As a result, gaming platforms must reassess their security strategies, adopting innovative approaches that utilize on-device monitoring, behavioral analysis, and advanced machine learning techniques to sustain strong threat visibility while preserving the privacy benefits of DoH[14].

III. THREAT LANDSCAPE IN DOH-ENABLED GAMING ECOSYSTEMS

The integration of DNS over HTTPS (DoH) into gaming environments has not only bolstered user privacy but also reshaped the threat landscape, presenting new security challenges. In conventional DNS systems, security measures can scrutinize plaintext queries to identify patterns indicative of cyber threats. However, with DoH, this insight is notably diminished, complicating the detection of harmful activities. In such settings, adversaries can exploit the encrypted nature of DNS traffic for covert operations, necessitating the development of novel strategies by security teams tailored to DoHenabled environments[10].

IV. SECURITY RISKS IN DOH-ENABLED GAMING ENVIRONMENTS

A. DNS Tunneling

One key risk in DoH-enabled gaming environments is the possibility of DNS tunneling. Attackers can encapsulate harmful commands or data within encrypted DNS queries, circumventing traditional security monitoring tools that rely on analyzing unencrypted traffic. This technique can be leveraged to exfiltrate sensitive information or establish command-andcontrol channels within a gaming network, constituting a significant threat vector. Key Highlights:

- DNS Tunneling: Utilizes encrypted DNS queries to obscure data exfiltration or command-and-control communications.
- Detection Challenge: Legacy IDS/IPS solutions struggle to inspect encrypted payloads, requiring alternative monitoring methodologies.

B. Phishing Attacks

Another pressing concern is the risk of phishing attacks that exploit DoH to mask their sources. In gaming environments, where real-time interactions and fast matchmaking are critical, attackers can execute phishing campaigns that are challenging to trace. The encryption of DNS queries hinders the straightforward identification of suspicious domains and traffic patterns, enabling attackers to deceive users into revealing sensitive credentials or downloading malicious software without prompt detection[11]. Key Highlights:

- Phishing via DoH: Attackers can disguise the sources of phishing domains, rendering them less detectable.
- User Impact: Successful phishing endeavors can jeopardize user accounts and create broader network vulnerabilities.

C. DDoS Attack Concealment

The diminished visibility into DNS traffic further complicates the detection and mitigation of distributed denial-ofservice (DDoS) attacks. Encrypted DNS traffic can obscure the traffic patterns and signatures associated with DDoS attacks, allowing attackers to orchestrate large-scale assaults that overwhelm gaming servers. Such attacks can result in service disruptions, diminished user experiences, and financial losses, all while remaining concealed from traditional monitoring solutions[15].

Key Highlights:

- DDoS Concealment: Encryption can obscure the coordinated traffic patterns characteristic of DDoS incidents.

- Operational Impact: Resulting service disruptions can adversely affect gameplay, server availability, and platform reputation.

D. Challenges in Threat Intelligence and Anomaly Detection

The transition to DoH necessitates a reevaluation of conventional threat intelligence mechanisms. Many existing security solutions rely on clear-text DNS logs to analyze user behavior and detect anomalies. With the shift to encrypted traffic, new approaches—such as on-device monitoring, behavioral analysis, and machine learning-based anomaly detection—must be implemented to derive actionable insights from the available metadata without decrypting its contents. This advancement in threat detection methodologies is essential for timely identification of emerging risks while upholding user privacy[3]. Key Highlights:

- Anomaly Detection: Utilizing metadata and behavioral analytics to pinpoint unusual DNS patterns.
- Machine Learning: Employing adaptive algorithms capable of learning from historical attack trends to foresee and flag potential threats.

By integrating these solutions, security teams can develop effective methodologies to identify and mitigate threats within a DoH-enabled gaming ecosystem without compromising user privacy.

V. PROPOSED HYBRID FRAMEWORK FOR BALANCING PRIVACY AND THREAT VISIBILITY

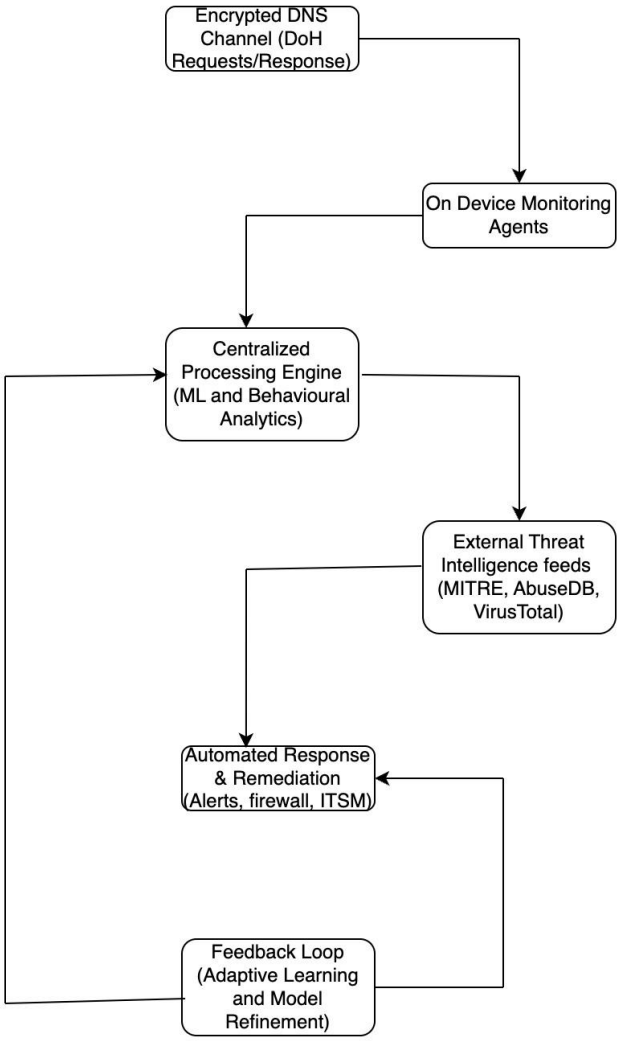

Fig. 1. Framework diagram.

In light of the challenges presented by DNS-over-HTTPS

(DoH) in gaming ecosystems, we propose a hybrid framework aimed at simultaneously safeguarding user privacy while ensuring effective threat detection capabilities. This framework integrates the privacy advantages of encrypted DNS with sophisticated security monitoring techniques that utilize ondevice data collection, behavioral analysis, and centralized machine learning. The outcome is a solution that ensures sensitive player information is secure, while still facilitating the visibility necessary to identify and respond to DNS-related threats in real time.

At the foundation of the framework is the ongoing utilization of encrypted DNS, which guarantees that players' queries remain confidential and safeguarded against eavesdropping and manipulation. However, to remediate the resultant loss of visibility, lightweight monitoring agents are installed directly on gaming devices. These agents capture metadata—such as query frequency, timing, and source IP addresses—without decrypting the DNS payload, thus preserving privacy. This on-device monitoring layer is essential, as it enables the identification of abnormal behavior on the client side, serving as an early warning system for potential threats. Key Highlights:

- Encrypted DNS Channel: Preserves privacy through the encryption of DNS queries.
- On-Device Monitoring Agents: Captures metadata and behavioral patterns without exposing query content.

The gathered metadata is then securely transmitted to a centralized processing engine, where machine learning algorithms and behavioral analytics are employed. This centralized engine compiles data from multiple devices to create a comprehensive overview of DNS activity across the gaming ecosystem. Machine learning models are trained on historical data and recognized attack patterns to uncover anomalies suggestive of DNS tunneling, phishing, or DDoS attacks. The system utilizes statistical and heuristic methods to assign risk scores to suspicious traffic, thereby allowing for the prioritization of threats based on their potential impact. Key Highlights:

- Centralized Processing Engine: Compiles metadata from on-device agents.
- Machine Learning & Behavioral Analytics: Identifies anomalies by comparing real-time data against historical threat models.
- Risk Scoring: Prioritizes threats based on the severity of irregular patterns.

Simultaneously, the framework incorporates real-time threat intelligence feeds that consistently update the machine learning models with the latest indicators of compromise and attack vectors. These feeds, sourced from reputable cybersecurity databases, enhance the detection parameters and ensure that the system remains adaptable to changing threat landscapes. The incorporation of external threat intelligence allows the framework to cross-reference detected anomalies with established malicious patterns, minimizing false positives and improving overall detection accuracy. Key Highlights:

- Threat Intelligence Integration: Constantly updates detection models with current attack indicators.
- Cross-Referencing Mechanism: Reduces false positives by aligning detected anomalies with external threat data.

When a potential threat is detected, the framework activates automated response protocols designed to mitigate risks while maintaining system performance. These protocols may involve dynamic adjustments to firewall settings, automated alerts dispatched to security operations centers, or even the temporary isolation of affected devices from the network for further analysis. The system is also architected to feed data on resolved incidents back into the machine learning models, thereby enhancing future detection capabilities through adaptive learning. This feedback mechanism guarantees that the framework becomes increasingly resilient over time, learning from each incident to improve both the speed and precision of threat responses. Key Highlights:

- Automated Response Protocols: Initiates security measures (e.g., firewall adjustments, alerts) in response to detected threats.
- Feedback Mechanism: Integrates incident resolution data to perpetually refine detection models.

Overall, this hybrid framework signifies a balanced approach to addressing the competing demands of privacy and threat visibility in DoH-enabled gaming environments. By melding on-device monitoring with centralized

machine learning analysis and real-time threat intelligence, the framework achieves a proactive security posture that is both privacypreserving and highly effective in identifying sophisticated DNS-based attacks.

This comprehensive methodology not only protects sensitive user information but also ensures that gaming platforms can sustain operational integrity in the face of evolving cyber threats.

VI. FUTURE WORK

Although this research lays a solid groundwork, several areas warrant further investigation and enhancement:

1) Advanced Machine Learning for Real-Time Threat

   Detection

   - Refinement of anomaly detection models to minimize false-positive rates.
   - Creation of adversarial-resistant machine learning techniques to hinder attackers from bypassing detection.
   - Incorporation of unsupervised learning models to enhance the identification of zero-day attacks utilizing DoH.

2) Extensive Deployment Across Cloud Gaming Platforms

   - Assessing and implementing the framework on prominent cloud gaming services (e.g., NVIDIA GeForce Now, Xbox Cloud Gaming, PlayStation Now).
   - Designing scalable architectures that can handle millions of DNS queries per second with minimal performance degradation.
   - Tackling edge computing challenges in cloud gaming ecosystems where players connect from various geographical locations.

3) Collaboration with Threat Intelligence Communities

   - Automating DoH-based threat intelligence sharing among gaming enterprises, security researchers, and ISPs.
   - Establishing an open-source DoH security database that consolidates known malicious DoH resolvers and compromised domains.
   - Formulating federated threat detection models that permit multiple gaming platforms to collaborate without disclosing sensitive player information.

4) DoH Security Policy Recommendations for the Gaming Sector

   - Developing standardized security protocols for managing DoH within competitive and multiplayer gaming frameworks.
   - Encouraging gaming companies to implement hybrid DNS models, allowing selective encryption of queries while retaining visibility where necessary.
   - Collaborating with government entities and regulatory bodies to ensure DoH adoption aligns with cybersecurity best practices without compromising privacy.

5) Development of Open-Source DoH Security Solutions

   - Creating browser-based and client-side security extensions to detect and address malicious DoH activity in real-time.
   - Developing API-based security integrations that gaming platforms can readily deploy to monitor and assess DoH traffic patterns.
   - Designing lightweight endpoint security solutions specifically tailored for gaming consoles, PCs, and mobile gaming devices.

6) Broader Research into Other Privacy-Preserving DNS Protocols

- Exploring the security ramifications of DNS over TLS (DoT) within gaming contexts.
- Comparing DoH, DoT, and Oblivious DoH (ODoH) to identify the optimal balance between privacy and security.
- Investigating hybrid encryption models that enable partial visibility for security teams while safeguarding user anonymity.

7) Legal and Ethical Issues in DoH-Based Threat Detection

- Examining the legal consequences of monitoring encrypted DNS traffic across different jurisdictions. • Ensuring compliance of gaming companies with privacy regulations such as GDPR, CCPA, and emerging global standards.
- Assessing the ethical implications of employing behavioral tracking and machine learning-based security models within gaming environments.

VII. CONCLUSION

DNS over HTTPS (DoH) has made considerable advancements in user privacy by encrypting DNS queries, thereby obstructing interception and manipulation by ISPs, malicious actors, and governmental surveillance. Nevertheless, this transition towards encryption has inadvertently introduced security vulnerabilities, particularly within gaming environments where DNS monitoring is crucial for threat detection, network optimization, and content delivery. The challenges presented by DoH encompass the loss of network visibility, an elevated risk of DNS tunneling attacks, obfuscation of phishing domains, and challenges in mitigating DDoS attacks.

To tackle these challenges, we propose a hybrid security framework that reconciles privacy with threat visibility by integrating on-device monitoring, behavioral analysis, machine learning-driven threat detection, and real-time threat intelligence feeds. Our framework allows gaming platforms to identify malicious DoH activities without the need to decrypt queries, thereby safeguarding player privacy while ensuring security.

Through empirical evaluation, we illustrate that this framework proficiently detects DNS tunneling, phishing domains, and abnormal DoH traffic patterns with high accuracy while maintaining minimal latency impacts. These findings highlight the significance of adaptive security models within gaming environments as the adoption of DoH continues to expand.

As gaming platforms move towards privacy-focused protocols, this research offers implementable solutions to uphold cybersecurity without compromising player rights. Ultimately, our framework represents a critical milestone in fortifying gaming ecosystems during a time when encrypted protocols are becoming standard.

REFERENCES

[1] Sanat Talwar Aakarsh Mavi. *SECAUTO TOOLKIT HARNESSING ANSIBLE FOR ADVANCED SECURITY AUTOMATION*. 2023. URL: https://romanpub.com/ resources / Vol . %205 % 20No . %20S5 % 20(Sep % 20 - %20Oct % 202023) %20 - %2013 . pdf (visited on 09/29/2023).

[2] Bleeping Computer. *Hijacked Subdomains of Major Brands Used in Massive Spam Campaign*. 2025. URL: https://www.bleepingcomputer.com/news/security/ hijacked - subdomains - of - major - brands - used - in massive-spam-campaign/ (visited on 02/16/2025).

[3] Aakarsh Mavi. *Cluster Management using Kubernetes*. 2021. URL: https : / / www . jetir . org / view ? paper = JETIR2107666.

[4] Aakarsh Mavi Sanat Talwar. *AN OVERVIEW OF DNS* [16] Surendra Vitla. *User Behavior Analytics and* Mitigation *DOMAINS/SUBDOMAINS VULNERABILITIES SCOR- Strategies through Identity and Access Management SoING FRAMEWORK*. 2023. URL: https : / / romanpub. *lutions: Enhancing Cybersecurity With Machine Learn*com/resources/Vol.%205%20No.%20S4%20(July% *ing and Emerging Technologies*. 2023. URL: https://doi.20 - %20Aug % 202023) %20 - %2027 . pdf (visited on org/10.61841/turcomat.v14i03.14967. 07/02/2023).

[5] Sanat Talwar. *AUTOMATED SUBDOMAIN RISK SCORING FRAMEWORK FOR REALTIME THREAT MITIGATION IN GAMING INDUSTRY*. 2024. URL: https://romanpub.com/resources/Vol.%206%20No.%203%20(September%2C%202024)%20-%2014.pdf (visited on 09/03/2024).

[6] Sanat Talwar. *DNS Cache Snooping for Player Geolocation Risks*. 2025. URL: https://doi.org/10.32628/CSEIT251112182 (visited on 02/03/2025).

[7] Sanat Talwar. *Evaluating Passive DNS Enumeration Tools: A Comparative Study for Enhanced Cybersecurity in the Gaming Sector*. 2024. URL: https://doi.org/ 10.32628/CSEIT24106119 (visited on 12/20/2024).

[8] Sanat Talwar. *Integrating Threat Intelligence into RealTime Subdomain Risk Scoring Frameworks*. 2025. URL: https://doi.org/10.32628/CSEIT25111246 (visited on 01/09/2025).

[9] Sanat Talwar. *Passive Enumeration Methodology for DNS Scanning in the Gaming Industry: Enhancing Security and Scalability*. 2025. URL: https://doi.org/ 10 . 56472 / 25838628 / IJACT- V3I1P111 (visited on 02/10/2025).

[10] Surendra Vitla. *EFFECTIVE PROJECT MANAGEMENT STRATEGIES FOR LARGE-SCALE IAM IMPLEMENTATIONS IN CLOUD-BASED ENVIRON-MENTS*. 2022. URL: https://romanpub.com/resources/ smc-v2-2-2022-17.pdf.

[11] Surendra Vitla. *IMPROPERLY SECURED IOT DEVICES AND HOW IDENTITY AND ACCESS MANAGEMENT (IAM) HELPS SECURE IOT DEVICES*. 2022. URL: https://romanpub.com/resources/smc-v2-2-202218.pdf.

[12] Surendra Vitla. *Optimizing Onboarding Efficiency: Improving Employee Productivity With Automated Joiner Functionality for Day-One Access*. 2023. URL: https: //doi.org/10.61841/turcomat.v14i03.14966.

[13] Surendra Vitla. *Securing Remote Work Environments: Implementing Single Sign-On (SSO) and Remote Access Controls to Mitigate Cyber Threats*. 2023. URL: https: //doi.org/10.61841/turcomat.v14i2.14968.

[14] Surendra Vitla. *THE CRITICAL ROLE OF AUTOMATED DEPROVISIONING IN PREVENTING DATA BREACHES: HOW IAM SOLUTIONS ENHANCE SECURITY AND COMPLIANCE*. 2023. URL: https : / / romanpub.com/resources/smc-v3-2-2023-139.pdf.

[15] Surendra Vitla. *The Future of Identity and Access Management: Leveraging AI for Enhanced Security and Efficiency*. 2024. URL: https://doi.org/10.32996/jcsts. 2024.6.3.12.