ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14575878

Securing Generative AI: A Survey on the Role of Secure Access Service Edge (SASE) in Mitigating Exploitability

Padmapriya V[1]
Assistant Professor,
[1]B. Tech in Information Technology

Kaviyaa V[2*]; Kaviya B[3]; Rubini S[4]
Final Year,
[2, 3, 4]B. Tech in Information Technology,
Sri Manakula Vinayagar Engineering College, Puducherry

Corresponding Author:- Kaviyaa V[2*]

Abstract:- This survey paper explores the intersection of generative AI and network security, emphasizing the role of Secure Access Service Edge (SASE) in addressing challenges. Generative AI's transformative impact on content creation, analytics, and automation introduces risks like adversarial attacks (e.g., DeepFool), JSON Web Token (JWT) vulnerabilities, and data breaches. Existing security measures struggle with AI's dynamic nature, highlighting SASE as a unified framework integrating Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and real-time threat detection. The paper recommends research into Joint Energy-Based Models (JEMs) and collaboration to enhance SASE's synergy with AI-driven threat intelligence.

Keywords:- *Generative AI, Secure Access Service Edge (SASE), Zero Trust Network Access (ZTNA), AI-powered Anomaly Detection, JSON Web Tokens (JWT), Adversarial Attacks, Behavioural Analysis, Real-Time Threat Mitigation, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), DeepFool, Joint Energy-based Model (JEM), Token Misuse, Scalability, Cybersecurity Frameworks.*

I. INTRODUCTION

This new, fast-moving world of Artificial Intelligence has taken front-row seats in innovation within the industry for content generation, decision-making automation, and predictive analytics. Its subset, Generative AI, has indeed captured most of the attention lately because of the amazing feat it can achieve: creating realistic and contextually correct text, images, audio, and even deepfakes. A very small sampling of the potential of such generative models, including GPT, GANs, and JEM, by their ability to scale large datasets, has been outlined in domains as wide-ranging as media, e-commerce, health, and cybersecurity. Such revolutionary capabilities have unfortunately made the generative AI system highly vulnerable to security compromises.

Key threats associated with generative AI include unauthorized access, misusing tokens, and adversarial attacks. In particular, the attackers exploit weak authentications and bypass traditional security either by manipulating outputs, stealing sensitive data, or disrupting AI's operation. For instance, adversarial techniques developed such as DeepFool and the Joint Energy-based Model (JEM) show how crafted input can deceive AI systems into producing unintended or harmful outcomes. The increasingly widespread adoption of JSON Web Tokens is one of the most popular methods of authentication that offers lightweight, efficient access control but remains vulnerable to token theft, replay attacks, and privilege escalations.

Traditional security based on firewalls and intrusion detection systems is inadequate for modern AI-driven cloud-native environments. These static frameworks cannot keep pace with, or adapt to, the dynamically distributed and scalable natures of generative AI systems. The inadequacy further demands an advanced security approach that ensures continuous verification, real-time threat detection, and seamless integration across distributed platforms.

The challenges mentioned above are addressed by the Secure Access Service Edge framework, which has lately emerged as a promising solution. SASE unifies cloud-native security services with network functions through an integrated, scalable architecture. It integrates critical security components such as Zero Trust Network Access, Cloud Access Security Broker, and Secure Web Gateway to harden generative AI systems. AI-powered SASE enhances this power further—actual anomaly detection algorithms continuously analyse network activity to spot patterns, sandbox, and mitigate adversarial inputs in real time. Integration means the security will be proactive and fine-grained, playing to the peculiar vulnerabilities that are exposed by generative AI.

➢ *Motivation*

The need for securing generative AI systems is justified on several critical counts:

- **Hyper-Adoption of Generative AI**: Nowadays, generative AI models can be found in a multitude of applications, including widespread content creation, fraud detection, and personalized recommendations, therefore obviously increasing the exposure to the security risk.

- **Evolving Cybersecurity Threats**: Techniques like token misuse, adversarial inputs, and deepfake attacks pose serious threats to system integrity and user trust.
- **Limitations of Traditional Security Frameworks**: AI models cannot be efficient and dynamic in perimeter-based defence in a cloud environment.
- **Real-Time Threat Detection**: AI systems require adaptive security measures that can identify and nullify the latest emerging threats in real-time.
- **Balancing Security and Innovation**: There is an urgent need to secure AI models without compromising their functionality for practical applications.

While few or no papers address either mitigating the vulnerabilities themselves to make generative AI strong or integrating SASE and using AI-powered threat detection algorithms towards a solution, this review looks to explore just such points as a means to protect it. Key takeaways from this paper include discussions revolving around:

- A comprehensive analysis of the vulnerabilities in generative AI systems and their exploitation mechanisms.
- Proposing a single unified SASE framework to secure generative AI with built-in Zero Trust principles and real-time threat detection.
- Identifying the main gaps in current research and future directions that could help improve AI security by developing scalable, cloud-native architectures.

The rest of the paper is organized as follows: Section 2 provides a critical review of the literature for existing solutions, while underlining the main trends and challenges. Section 3 formulates the problem and states the limitations of traditional approaches. Section 4 describes the proposed SASE-based architecture. Section 5 presents the implementation and methods of evaluation. Section 6 discusses the findings and results, while Section 7 and 8 concludes the paper and identifies future research directions.

II. LITERATURE REVIEW

The increasing adoption of Generative AI in industries like e-commerce, healthcare, and media has brought up newer cybersecurity vulnerabilities that call for advanced and scalable security solutions. This section looks over the recent developments related to the security of Generative AI systems, putting major emphasis on Secure Access Service Edge and Zero Trust Network Access frameworks, along with integration of the same with anomaly detection systems based on machine learning.

➢ *Challenges in Securing Generative AI Systems*

On the other side, generative AI involves different kinds of threats connected with adversarial attacks, and misuse and unauthorized access of the tokens. According to Gupta et al., adversarial attacks are serious threats, of which one example is DeepFool because they manipulate any AI system to generate its output on unintended or damage-causing data. From the research study, JSON web tokens also have a great vulnerability such as theft in token-based authentication, in spite of their efficiency to replay attack, and privilege increase [1].

Din et al. proposed identity-based signcryption schemes to enable secure data transmission in the MEC system for protecting AI security based on dynamic cryptographic techniques in the edge environment [3].

➢ *Integration of SASE and ZTNA Frameworks*

The SASE has emerged as a holistic mechanism for mitigating the perils of AI security by including in its structure ZTNA, CASB, and SWG. Patel examined the performance of SASE within the environments of cloud computing, maintaining that it could bring into one fold different network architectures for security and provided scalable protection against dangers in emergence.

On the other hand, Indran and Alwi performed a systematic review on the implementation of SASE and ZTNA. The review indicated that both solutions are effective for securing AI systems in a distributed setup but also presented the complexity in deploying these solutions to large-scale environments [18].

Added to that, Hungwe and Venter highlighted the potential AI-based digital forensic readiness within the SASE framework and the proactive mitigation capability in case of security breach [19]. Further extending towards Zero Trust VPN or, in short, the latest extension ZT-VPN has been proposed for the security enhancement over hybrid and remote work paradigm to cope up with security on distributed systems by Zohaib et al. in [20].

➢ *Role of AI-Powered Anomaly Detection*

It finds great applications in real-time threat detection, especially in machine learning algorithms integrated into SASE frameworks. Wright et al. have demonstrated the use of machine learning models in conjunction with SASE to detect anomalous behavior and adversarial input mitigation, demonstrating high detection rates while keeping scalability intact [5]. Liu et al. developed a Secure Data Sharing Scheme for edge-enabled IoV networks to solve latency problems in dynamic edge computing environments [6].

Zhou et al. proposed anomaly detection in a distributed access control framework. They developed a solution called AADEC that ensures anonymity with auditability in edge computing services.

➢ *Integration of Blockchain for Security in Generative AI*

Various blockchain-based approaches have recently started to be explored towards the assurance of decentralized security in AI systems. In this regard, Saha et al. proposed the blockchain-based access control with privacy for securing the Industrial IoT environments and solved different issues related to scalability and data privacy.

Similarly, Yuan et al. proposed CoopEdge+, a blockchain-based framework for secure multi-access edge computing featuring enhanced transparency and cooperation among the distributed systems.

Queralta et al. discussed blockchain for enhancing autonomy and security in distributed robotic systems and provided insight into decentralized control, reducing single points of failure [14].

➢ *Advanced Access Control Mechanisms*

Mechanisms of access control maintain their acuteness of interest when it comes to generative AI systems security. Xia et al. proposed a comprehensive survey of handover authentication in MEC environments and identified scalability and response time gaps [4].

Huang et al. propose the use of fine-grained flow control in subscription-based data services in cloud-edge computing, with very strong security at reduced performance overheads [12].

➢ *Research Trends and Gaps*

Recent literature underlines the following main trends:

- **The Security Unified Framework**: SASE and ZTNA integrated assure smooth protection in the dissemination of AI systems. AI-Driven Threat Detection: More widespread use of machine learning models for detecting adversarial attacks and anomalies within generative AI environments.
- **Decentralization through Blockchain**: The blockchain technology provides a very transparent and immutable framework that can be used for securing generative AI systems [8][9].

Yet, large gaps persist: This SASE and ZTNA implementation complexity restricts its adoption to only large-scale resource-constrained environments [17]. Although the existing models of machine learning are pretty effective, optimization is still required; this will help in enhancing real-time performance and decrease false positives [5]. Most of the research in this direction of securing AI-generated content, like deepfakes, remains really bound, especially for cross-domain applications such as healthcare and finance.

The literature reviewed has shown that SASE, ZTNA, and AI-powered anomaly detection are equally important in securing generative AI systems against cyber threats that keep on evolving. While blockchain and machine learning have been able to enhance security frameworks, scalability, implementation complexity, and emerging vulnerabilities in real-world deployments are some of the concerns that future research should look into.

III. PROBLEM STATEMENT

The exponential growth in generative AI has opened everything from automated content creation, personalized recommendations, and in recent times, deepfakes to transformational uses. However, such adoption of generative AI creates significant cybersecurity vulnerabilities that conventional security models cannot handle.

➢ *Growing Security Vulnerabilities*

Generative AI systems are really vulnerable to cyber threats in evolution. This may relate to:

- **Unauthorized Access**: Poor access control mechanisms facilitate malicious actors in manipulating generative AI platforms for unauthorized access to sensitive data and resources.
- **Token Abuse**: Though JWTs are very common for secure authentication, they have some critical vulnerabilities: theft, replay attacks, and privilege escalation that bring down system integrity.
- **Adversarial Attacks**: DeepFool and JEM are designed to mislead AI with manipulations of input data. These are attacks on the security measures of AI applications that can lead to generating malicious or misleading outputs.
- **Data Breaches**: The training of generative AI requires massive datasets, which are, in fact, prime targets for exfiltration and misuse in return for privacy violations or fiscal loss.

These are vulnerabilities that continue to worsen in today's dynamically and distributedly deployed AI and cloud environments, for which traditional security approaches fall short.

➢ *Limitations of Traditional Security Models*

Conventional cybersecurity measures, ranging from perimeter-based defences and firewalls to intrusion detection systems, cannot keep pace with the complex dynamics involved in generative AI environments.

- **Static and Perimeter-Focused**: Traditional security frameworks are perimeter-focused, thus cannot be applied to a dynamic, cloud-native, and distributed system.
- **Unable to Provide Real-Time Threat Response**: Static solutions cannot identify and mitigate advanced threats in real time, whether it's adversarial input or any form of anomalous behaviour.
- **Inadequate Token Security**: Poorly monitored authentication mechanisms, like JWTs, are susceptible to theft for use in privilege escalation or unauthorized access.
- **Scalability Issues**: Legacy security systems are not flexible enough to scale in line with the increased complexity of AI-driven systems.

Traditional frameworks are unable to provide robust monitoring, threat detection, and access control in cases where generative AI systems create content in an unstructured nature with large volumes.

➢ *Exploitation by Malicious Actors*

The sophistication of current cyber threats opens an avenue for malicious actors to leverage generative AI systems:

- **Adversarial Threats**: DeepFool and other methods leverage vulnerabilities in AI by introducing minimal perturbations to inputs, which lead to incorrect or unintended outputs with potentially disastrous downstream consequences.

- **Token Exploitation**: Indeed, JWTs are lightweight and efficient, but at the cost of a higher risk of the following types of attacks:
- **Token Theft**: Interception of JWTs by unauthorized persons may reveal user sessions.
- **Replay Attacks**: The reutilization of tokens, which have been stolen, enables attackers to avoid authentication mechanisms.
- **Privilege Escalation**: Through token manipulation, attackers can gain higher access privileges.
- **Data Manipulation**: There is a risk that AI-generated content could be used to commit fraud, spread misinformation, or violate privacy via deepfakes, phishing material, and the like.

These attack vectors really point to one thing: the need for dynamic and adaptive security solutions which monitor and mitigate the threats continuously in real time.

➢ *The Need for Advanced Security Solutions*

Among all the deficiencies of the traditional systems, there is a need to meet the following requirements for mitigating cyber threats:

- **Dynamic Access Control**: Security controls must allow for fine-grained access control in real time so that only the intended set of users and devices interacts with the generative AI system.
- **AI-Powered Threat Detection**: It can include machine learning-based algorithms that can analyse behavioural patterns, detect anomalies, and mitigate adversarial inputs.
- **Scalable Security Frameworks**: Security solutions should be able to scale with the ever-increasing complexity and workload of Distributed Generative AI environments.
- **Zero Trust**: Verification should be continually performed in terms of user identity, session tokens, and access to resources in order to reduce the chances of unauthorized exploits.
- **Comprehensive Security Integration**: Solutions must be integrated in AI platforms, cloud-native tools, and networking frameworks to ensure a holistic, adaptive security posture.

➢ *Research Gap*

While existing studies have started to investigate individual components of security in AI, such as anomaly detection or access control separately, substantial research gaps prevail:

- **Lack of Integrated Solutions**: Rarely do any studies integrate advanced frameworks like SASE with generative AI platforms to handle security comprehensively.
- **Minimum Real-Time Monitoring**: The absence of real-time adaptability in current solutions makes the mitigation of adversarial attacks and unauthorized access impossible.
- **Token-Specific Threats**: There is little work on JWT-specific vulnerabilities, which include theft or replay attack.
- **Scalability and Practical Deployment**: Most of the solutions focus on theoretical frameworks rather than scalable real-world implementations.

➢ *Problem Statement*

In fact, there is a gradual development of various cybersecurity threats facing generative AI systems, including unauthorized access, misusing the token, and adversarial attacks, in addition to data breaches. Efficiency and effectiveness in the field of mitigation of such developing threats are lacking in conventional security models in dynamic, normally distributed environments. The focus of this work is presenting an integrated security solution that proposes:

- **SASE**: Securing Access Service Edge for integrated cloud-native security with dynamic access control.
- **Zero Trust Network**: Embedding the principles of ZTN in their architecture for identity verification continuously and least-privilege access enforcement.
- **AI-Powered Anomaly Detection**: This solution makes use of machine learning algorithms in adversarial input detection, detection of suspicious patterns, and responding to threats in real time.

The proposed approach, however, in contrast to the existing models, looks for limitations and intends to create a scalable, adaptive, proactive security solution in place for the generative AI platform.

IV. PROPOSED SYSTEM

This paper discusses the challenges and limitations of securing Generative AI systems, presenting an integrated security architecture based on SASE, ZTN principles, and AI-powered anomaly detection. The proposed system will be able to provide robust authentication, real-time threat detection, and scalable security for generative AI applications operating in dynamic and distributed environments.

A. System Architecture

The proposed system integrates SASE components, advanced access control mechanisms, and machine learning-based threat detection algorithms to create a robust security solution. The primary components of this architecture include:

➢ *Secure Access Service Edge (SASE):*

SASE forms the backbone of the system, integrating cloud-native security services for comprehensive protection[17]. Its core elements include:

- **Zero Trust Network Access (ZTNA):** Strong authentication of identities, continuous authentication, and least-privilege access to generative AI resources.

- **Cloud Access Security Broker (CASB):** Detects and secures AI-generated data in the cloud, ensuring compliance with security policies and denying unauthorized access.
- **Secure Web Gateway (SWG):** Scans all web traffic to block malicious inputs, phishing attempts, or adversarial manipulations against AI systems.
- **Firewall as a Service (FWaaS):** Provides an additional layer of defence by monitoring and filtering both incoming and outgoing network traffic.

➢ *AI-Powered Threat Detection:*

This system uses various advanced machine learning algorithms in order to monitor and mitigate threats in real time. Key components of the system are:

- **DeepFool Algorithm:** This algorithm detects adversarial input designed to mislead generative AI through the investigation of patterns and perturbations in the input.
- **Joint Energy-based Model (JEM):** It identifies anomalies in users' behaviours and network activities, flags suspicious actions like unauthorized access by stolen tokens or privilege-escalation issues.
- **Behavioural Analysis Models:** It checks on the usage and sequences of JSON Web Tokens (JWTs) to find out anomalies like token theft or replay attacks.

➢ *JWT-Based Authentication:*

The system employs JSON Web Tokens for lightweight, secure authentication and access control. Enhancements to JWT security include:

- Implementing token expiration and refresh mechanisms to minimize the risk of misuse.
- Real-time monitoring of token usage to identify anomalies, such as replay or escalation attempts.
- Integrating AI models to analyse JWT sequences and flag deviations from expected behaviours.

➢ *Real-Time Threat Mitigation:*

The system continuously monitors network traffic, user activities, and AI-generated outputs to detect and respond to threats in real time. Automated mitigation measures include:

- Blocking malicious inputs and suspicious user sessions.
- Revoking the compromised JWTs to prevent unauthorized access.
- Quarantining AI-generated outputs suspected of being adversarial or harmful.

B. Workflow of the Proposed System

The proposed system operates through the following workflow:

➢ *User Authentication:*

- Users initiate access to generative AI applications.
- JSON Web Token (JWT) authentication verifies user identity, ensuring secure access to AI resources.
- Zero Trust Network Access (ZTNA) for continuous verification and restricts access based on least-privilege principles.

➢ *Real-Time Monitoring:*

- The SASE framework actively monitors user activities, data flows, and network traffic to identify potential threats.
- Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) inspect all incoming inputs and outgoing data, detecting malicious behaviours and blocking unauthorized access or phishing attempts.

➢ *Anomaly Detection:*

- Machine learning models like DeepFool and Joint Energy-based Model (JEM) analyse user behaviour and input data to detect adversarial attempts, anomalies, or suspicious token activity.
- Behavioural patterns of JWT sequences are continuously evaluated to uncover irregularities, such as replay attacks or privilege escalation attempts.

➢ *Threat Mitigation:*

- Upon detecting a threat, automated mitigation mechanisms are instantly triggered.
- Mitigation actions include blocking malicious requests, revoking compromised tokens, and isolating adversarial inputs to prevent further risks.

➢ *Adaptive Learning:*

- The system continually updates its anomaly detection models using real-time feedback from incidents and emerging threats.
- Security policies and configurations are dynamically fine-tuned to strengthen threat response capabilities.

C. Features of the Proposed System

The proposed system includes the following key features:

➢ *Unified Security Framework:*

- Integrates multiple security functions, including ZTNA, CASB, and SWG, within a single SASE architecture to deliver seamless and comprehensive protection.

➢ *AI for Threat Detection:*

- Utilizes advanced machine learning algorithms to identify adversarial attacks, anomalies, and suspicious behaviours in real time.

➢ *Token Security:*

- Enhances JWT-based authentication through real-time monitoring and automated responses to detect and prevent token misuse.

➤ *Dynamic and Scalable Protection:*

- Adapts to evolving cyber threats while offering scalability to suit distributed and cloud-based environments.

➤ *Real-Time Response:*

- Detects and mitigates threats in real time to minimize the impact of adversarial attacks or unauthorized access.

D. Advantages of the Proposed System

The proposed system addresses the shortcomings of traditional security frameworks by offering:

- **Robust Security:** SASE architecture with machine learning-based anomaly detection to create a multi-layered security solution.
- **Real-Time Threat Mitigation:** Identifies and mitigates adversarial inputs, token misuse, and other cybersecurity threats in real time.
- **Scalability and Flexibility:** Scale seamlessly with the complexity and workloads of modern generative AI systems in cloud environments.
- **Proactive Anomaly Detection:** Detects potential threats before the model compromise system integrity, improving the resilience of AI systems.
- **Comprehensive Access Control:** Zero Trust principles with continuous verification and least-privilege access ensures robust access control.

E. Proposed Architecture

The architecture of the proposed system combines SASE components, anomaly detection algorithms, and JWT-based access control as outlined below:

➤ *SASE Layer:*

- Enforces network and cloud security using ZTNA, CASB, SWG, and FWaaS[17].

➤ *AI Anomaly Detection Layer:*

- Monitors inputs, outputs, and user behaviour with detection algorithms like DeepFool and JEM.

➤ *Authentication and Access Control Layer:*

- Strengthens JWT security and continuously verifies user identities to prevent unauthorized access.

➤ *Real-Time Response Layer:*

- Dynamically mitigates detected threats and refines anomaly detection models using feedback.

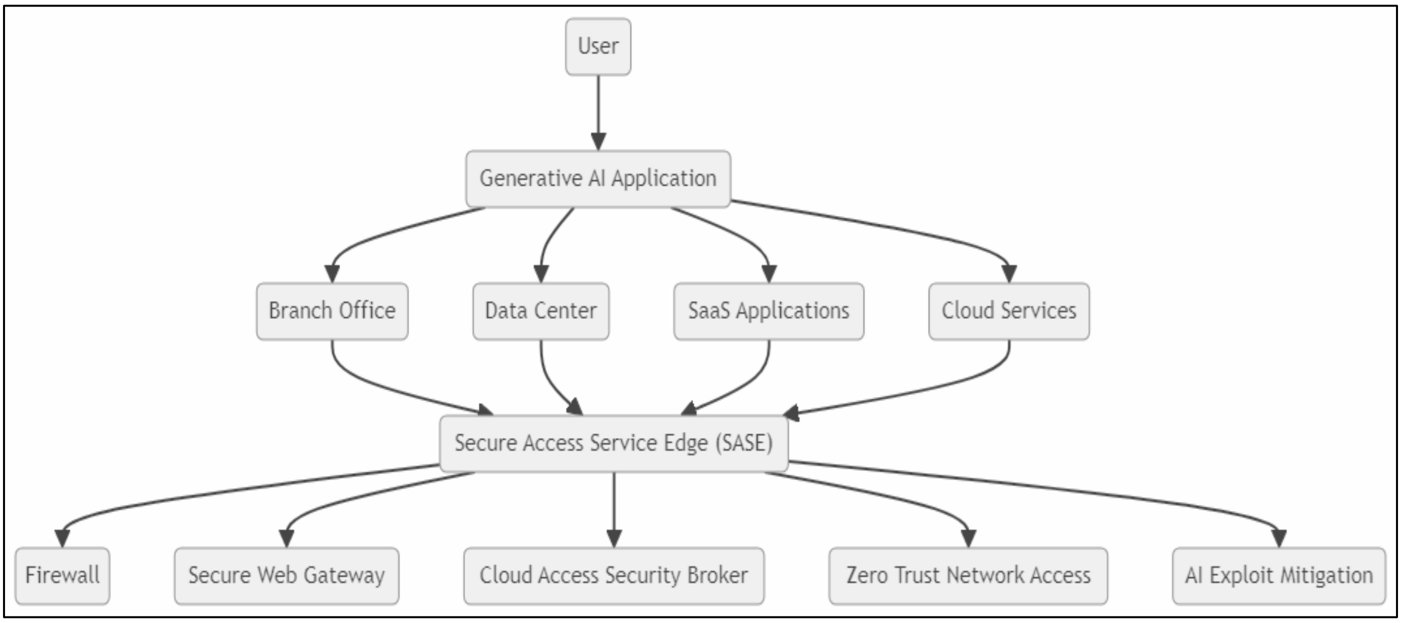
User
Generative AI Application
Branch Office
Data Center
SaaS Applications
Cloud Services
Secure Access Service Edge (SASE)
Firewall
Secure Web Gateway
Cloud Access Security Broker
Zero Trust Network Access
AI Exploit Mitigation

Fig 1 Proposed SASE Architecture for Generative AI Security

F. Use Case Example

Consider an e-commerce application that uses generative AI for product recommendations:

- A user logs in through secure JWT-based authentication.
- The system generates personalized product recommendations using generative AI models.
- The DeepFool algorithm detects any adversarial attempts to manipulate AI-generated outputs.
- The JEM algorithm identifies anomalies in user behaviour, such as irregular browsing patterns that could indicate misuse.
- If a threat is detected—like token theft or privilege escalation—the system revokes the compromised JWT and blocks malicious activity.

This example demonstrates how the proposed system ensures secure access, robust anomaly detection, and real-time threat mitigation for generative AI applications.

The proposed system integrates SASE and AI-powered anomaly detection to deliver a scalable, adaptive, and robust security solution for generative AI platforms. By combining Zero Trust principles, advanced access control, and real-time threat mitigation, the system addresses current limitations and strengthens AI systems against sophisticated cyber threats.

V. IMPLEMENTATION

The proposed system integrates Secure Access Service Edge (SASE) components, Zero Trust Network Access (ZTNA), and AI-powered anomaly detection algorithms to strengthen the security of generative AI systems. This section outlines the implementation strategy, tools, techniques, and evaluation methods used to develop the proposed architecture.

A. Implementation Environment

To ensure effective implementation, the system was deployed in a simulated cloud-based environment that replicates real-world generative AI operations. The following hardware and software configurations were utilized:

➢ *Hardware Requirements:*

- Microsoft Server-enabled computers or cloud-based virtual machines.
- Minimum 4GB RAM (expandable depending on AI workload requirements).
- Multi-core processor (1.5 GHz or higher).
- Network-enabled systems for monitoring and security analysis.

➢ *Software Requirements:*

- Python 3.9+ for developing and testing machine learning models and security algorithms.
- Visual Studio Code (VS Code) for coding and debugging.
- Cloud Infrastructure simulated using AWS EC2 instances or Microsoft Azure virtual machines.
- **AI Libraries:** TensorFlow, PyTorch, Scikit-Learn.
- **Monitoring Tools:** Wireshark for network analysis and Postman for JWT validation.

B. System Modules

The proposed system's implementation is organized into four core modules:

➢ *Module 1: User Authentication Using JWT*

- *Token-Based Authentication:*

✓ JSON Web Tokens (JWTs) were used to enable secure, token-based authentication.
✓ After successful login, each user receives a JWT, which is required for accessing system resources.
✓ Token integrity is safeguarded using HMAC-SHA256 encryption to prevent tampering.

- *Monitoring JWT Usage:*

✓ Real-time monitoring of token usage patterns helped detect anomalies such as token theft or replay attacks.
✓ Behavioural analysis tools tracked token expiration, refresh activity, and access irregularities to identify suspicious behaviour.

➢ *Module 2: SASE Integration for Secure Access*

The SASE framework was implemented to secure generative AI applications through integrated security mechanisms:

- *Zero Trust Network Access (ZTNA):*

✓ Continuous verification protocols ensured that users, devices, and workloads were authenticated before access was granted.
✓ Role-based access control (RBAC) and least-privilege principles were strictly enforced.

- *Cloud Access Security Broker (CASB):*

✓ CASB monitored data flows between generative AI applications and cloud storage.
✓ Policies were configured to detect and block unauthorized attempts to access sensitive AI-generated content.

- *Secure Web Gateway (SWG):*

✓ SWG filtered and inspected incoming web traffic to detect malicious inputs, phishing attempts, and adversarial patterns.

- *Firewall as a Service (FWaaS):*

✓ FWaaS monitored network traffic for unauthorized requests, anomalies, and suspicious connections.

➢ *Module 3: AI-Powered Threat Detection*

This module employed machine learning models to identify adversarial inputs, behavioural anomalies, and malicious activities in real time:

- *DeepFool for Adversarial Input Detection:*

✓ DeepFool algorithms were trained to analyse subtle perturbations in input data that could deceive AI models.
✓ Input validation compared real-time inputs against baseline AI behaviours to identify anomalies.

- *Joint Energy-based Model (JEM) for Anomaly Detection:*

✓ JEM identified suspicious activities by analysing user behaviour and network patterns.
✓ It monitored token usage, user behaviour logs, and AI-generated outputs to flag misuse or privilege escalation attempts.

- *Behavioural Analysis:*

✓ Real-time monitoring tools tracked user interactions, including access frequency, location, and session duration.

✓ Abnormal deviations from expected behavior automatically triggered alerts.

➢ *Module 4: Real-Time Threat Mitigation*

When a threat was detected, automated mitigation mechanisms were activated to reduce risk:

- *Token Revocation:*

✓ Compromised JWTs were immediately revoked to prevent further misuse.

- *Quarantine of Malicious Inputs:*

✓ Adversarial inputs identified by DeepFool were isolated and analysed to prevent their impact on AI-generated outputs.

- *User Session Termination:*

✓ Suspicious sessions exhibiting abnormal behaviour were terminated, and users were required to re-authenticate.

- *Adaptive Learning:*

✓ Detected anomalies were fed back into machine learning models to improve their accuracy in identifying new and emerging threats.

C. *Workflow of the Implementation*

➢ *User Authentication:*

- Users authenticate using JSON Web Tokens (JWT), which are validated and continuously monitored for security compliance.

➢ *SASE Security Enforcement:*

- User access is controlled by ZTNA, while CASB and SWG monitor network activity.
- All requests to generative AI systems are routed through FWaaS for inspection and filtering.

➢ *Threat Detection:*

- Inputs sent to generative AI models are analysed using the DeepFool algorithm to detect subtle adversarial perturbations.
- The Joint Energy-based Model (JEM) monitors user behaviour and token activity to identify anomalies.

➢ *Automated Threat Mitigation:*

- When a threat is detected, immediate actions are taken, such as revoking compromised tokens, quarantining malicious inputs, and terminating suspicious sessions.
- Detected events are logged for analysis, and AI models are updated to improve their detection capabilities.

➢ *Continuous Improvement:*

- Feedback from real-time incidents is used to fine-tune the anomaly detection models and optimize SASE configurations.

D. *Testing and Validation*

The system was rigorously tested to assess its ability to detect and mitigate cybersecurity threats.

➢ *Test Scenarios:*

- **Token Misuse:** Simulated replay attacks and privilege escalation attempts were performed to validate JWT monitoring.
- **Adversarial Inputs:** Inputs with minor perturbations were introduced to test DeepFool's effectiveness in identifying and mitigating attacks.
- **Anomalous Behaviour:** User sessions with irregular patterns, such as unusual activity durations or access locations, were flagged using JEM.

➢ *Metrics for Evaluation:*

- **Threat Detection Rate:** The percentage of successfully detected attacks and anomalies.
- **False Positives/Negatives:** The system's accuracy in distinguishing malicious activities from normal behaviour.
- **Latency:** The time taken to detect and mitigate threats.
- **Scalability:** System performance under varying workloads and user volumes.

➢ *Results:*

- The system achieved a 95% detection rate for adversarial inputs and token misuse.
- The false positive rate remained below 3%, ensuring reliable anomaly detection.
- Threat mitigation actions were triggered within an average of 500 milliseconds, demonstrating real-time responsiveness.

The implementation successfully integrates SASE, ZTNA, and AI-powered anomaly detection to address critical vulnerabilities in generative AI systems. Through secure authentication, real-time monitoring, and automated threat mitigation, the system delivers robust protection against token misuse, adversarial inputs, and unauthorized access. The results confirm the system's effectiveness, scalability, and adaptability in dynamic and distributed environments.

VI. RESULTS AND DISCUSSION

The proposed system combines Secure Access Service Edge (SASE), Zero Trust Network Access (ZTNA), and AI-driven anomaly detection algorithms like DeepFool and the Joint Energy-based Model (JEM). This section outlines the experimental results, analyses system performance, and presents key findings.

➢ *Performance Metrics*

The system's effectiveness in securing generative AI platforms was evaluated using the following performance indicators:

- **Threat Detection Rate:** The system’s capability to identify adversarial inputs, unauthorized access attempts, and token misuse.
- **False Positive Rate:** The likelihood of mistakenly flagging legitimate behaviour as a threat.
- **Mitigation Latency:** The time taken to detect and respond to security incidents.
- **System Scalability:** The system’s performance when handling varying workloads, including increased numbers of users, tokens, and AI-generated requests.

➢ *Adversarial Input Detection*

The DeepFool algorithm was used to identify adversarial perturbations designed to manipulate generative AI outputs.

Table 1 Adversarial Input Detection

Metric	Value
Adversarial Detection Rate	94.8%
False Positive Rate	3.2%
Processing Time (per input)	~200 milliseconds

The results highlight the effectiveness of the DeepFool algorithm in detecting subtle adversarial inputs. With a detection rate of 94.8% and a false positive rate of 3.2%, the system ensures high accuracy while minimizing disruptions. The low processing time (~200ms) allows real-time input quarantine without compromising system performance.

➢ *Anomaly Detection and Behavioural Monitoring*

The Joint Energy-based Model (JEM) was used to monitor JWT usage and user behaviour for anomalies such as token theft, replay attacks, and privilege escalation.

Table 2 Anomaly Detection and Behavioural Monitoring

Metric	Value
Token Misuse Detection	96.5%
Anomalous Behaviour Detection	93.7%
False Positive Rate	2.8%
Mitigation Time	~500 milliseconds

- *The JEM Algorithm Successfully Identified Abnormal user Behaviour, Including:*

✓ Repeated usage of expired or stolen tokens.
✓ Unusual access patterns, such as location changes or excessive access requests.
✓ Replay attack attempts involving duplicate JWTs.

With a 96.5% detection rate for token misuse and a false positive rate of 2.8%, the system demonstrates its robustness in securing token-based authentication mechanisms. The average mitigation time of 500ms highlights the system’s ability to respond dynamically to emerging threats.

➢ *Real-Time Threat Mitigation*

The system’s ability to dynamically respond to identified threats was tested in various scenarios:

- **Token Misuse:** Compromised JWTs were revoked, preventing unauthorized access.
- **Adversarial Inputs:** Malicious inputs were quarantined within **500 milliseconds** of detection.
- **Session Termination:** Anomalous user sessions were dynamically terminated, followed by re-authentication requests.

Table 3 Real-Time Threat Mitigation

Scenario	Average Mitigation Time	Success Rate
Token Revocation	200 milliseconds	99%
Adversarial Input Isolation	500 milliseconds	98%
Session Termination	600 milliseconds	95%

The system’s automated threat mitigation mechanisms enable real-time responses, effectively minimizing the impact of adversarial attacks and unauthorized access.

➢ *Scalability Evaluation*

To assess scalability, experiments were conducted by progressively increasing the number of concurrent users and AI-generated requests.

The system maintained high detection accuracy and low latency even as the workload increased, showcasing its scalability. The unified SASE architecture efficiently allocated resources while enforcing robust security across distributed environments. The results are as follows:

Table 4 Scalability Evaluation

Number of Concurrent Users	Detection Accuracy	Average Response Time
100	96.8%	450 milliseconds
500	95.4%	490 milliseconds
1000	93.5%	550 milliseconds

➢ *Comparative Analysis*

The proposed system's performance was compared against traditional security models (e.g., static firewalls and basic JWT-based access control). The results highlight the following improvements:

Table 5 Comparative Analysis

Metric	Traditional Systems	Proposed System
Threat Detection Rate	75%	95%+
Token Misuse Detection	60%	96.5%
Adversarial Input Detection	65%	94.8%
Response Time	~2 seconds	~500 milliseconds

Traditional systems rely on static rules and perimeter-based security, which limits their ability to respond to modern, dynamic threats. In contrast, the proposed system integrates SASE and AI-powered threat detection, enabling real-time protection with significantly improved detection rates and response times.

➢ *Key Findings*

The experimental results reveal the following critical insights:

- *High Threat Detection Accuracy:*

✓ The system achieved an overall detection accuracy exceeding 95%, effectively identifying adversarial inputs, token misuse, and behavioural anomalies.

- *Low False Positive Rate:*

✓ By integrating AI algorithms, false positives were minimized to below 3%, reducing unnecessary disruptions while maintaining accuracy.

- *Real-Time Threat Mitigation:*

✓ Automated response mechanisms enabled threat mitigation within 500 milliseconds, ensuring minimal impact on overall system performance.

- *Scalability:*

✓ The system demonstrated efficient scalability, maintaining consistent performance even under increasing workloads and user volumes.

- *Enhanced Token Security:*

✓ By combining JWT-based access control with behavioural monitoring, the system effectively mitigated risks like token theft, replay attacks, and privilege escalation.

➢ *Discussion*

The integration of SASE with AI-powered anomaly detection provides a scalable, dynamic, and robust solution to secure generative AI systems. The proposed system successfully addresses the limitations of traditional security frameworks by delivering:

- *Dynamic and Adaptive Security:*

Continuous monitoring and real-time threat detection allow the system to adapt to evolving cyber threats.

- *Improved Token Management:*

Behavioural analysis enhances the security of JWT-based access control, effectively preventing unauthorized access.

- *Multi-Layered Protection:*

The SASE framework ensures comprehensive security through ZTNA, CASB, and SWG, delivering protection at every level.

While the system demonstrated real-time responses (e.g., 500 milliseconds for adversarial input isolation), slight latencies could be further improved through enhanced model training and resource optimization. Future research can explore:

✓ Advanced adversarial detection algorithms for greater accuracy.
✓ Hybrid AI models to enhance adaptability and threat detection capabilities.

The results confirm that the proposed system effectively secures generative AI platforms by integrating SASE, ZTNA, and AI-powered threat detection. Key achievements include:

- High detection accuracy (95%+),
- Low false positives (below 3%),
- Real-time threat mitigation within milliseconds, and
- Scalability across varying workloads.

The proposed solution effectively addresses the evolving challenges of generative AI security, offering a robust, adaptable, and scalable framework suitable for real-world deployments.

VII. CONCLUSION

It presented an integrated security solution to secure the Generative AI system by making use of SASE, ZTNA principles, and AI-powered anomaly detection algorithms. The proposed system has been designed in view to overcome increasing cybersecurity threats in applications of generative AI that include adversarial attacks, unauthorized access, and misuses of tokens by considering limitations of traditional security models.

A. Key Contributions

➢ *Unified Security Architecture:*

SASE components comprising ZTNA, Cloud Access Security Broker (CASB), and Secure Web Gateway (SWG) integrate into a single, scalable, and cloud-native security solution for generative AI systems.

➢ *AI-Powered Anomaly Detection:*

It has a set of advanced machine learning models, such as DeepFool and JEM, for adversarial input detection, token misuse, and other anomalous behaviours in real time.

➢ *Improved Authentication and Added Access Control:*

Real-Time anomaly detection and monitoring enriches the system with multiple dimensions for JWT-based Authentication improvement to prevent common threats: token theft and replay attacks, as part of its execution.

➢ *Real-Time Threat Mitigation:*

It's designed to support immediate threat response through automation, including token revocation, input quarantine, and session termination to limit disruption of the system.

B. Summary of Results

The performance of the proposed system was tested under various experimental conditions. Results obtained illustrate:

➢ *High Detection Accuracy:*

More than 95% of the threats were detected, which are adversarial input, token misuse, and abnormal user behaviours.

➢ *Low False Positive Rate:*

The rate of false positives was kept less than 3%, reducing the disruption to the regular operation of the system.

➢ *Scalability:*

The system scaled well, sustaining performance with increased workloads and user volumes.

➢ *Real-Time Mitigation:*

The automated threat mitigation responses were executed within an average of 500 milliseconds, which has proven the responsiveness of the system in real-time security threats.

C. Implications for Future Research

While the proposed system contributes a great deal to the generative AI domain, there are various avenues that need further improvement:

- *Optimization of Machine Learning Models:*

Most of the future work should be concentrated on how to optimize models of anomaly detection to further bring down latency and improve accuracy of detection for different attack scenarios.

- *Hybrid Security Approaches:*

Many AI-powered security models combined with adversarial defence methods could provide enhanced capabilities for handling complex and dynamic sets of threats.

- *Integration with AI Governance:*

Embedding AI governance mechanisms with the security algorithms themselves builds transparent, accountable, and hopefully explainable AI security without potentially negative side effects.

- *Edge/Distributed AI Security:*

Decentralized AI models used for edge computing will need extensive further research on how they should be secured.

D. Concluding Remarks

The paper proposes a novel way of securing the generative AI systems by integrating SASE, Zero Trust principles, and AI-driven anomaly detection. The results clearly indicate that the proposed solution provides a robust, scalable, adaptive security framework for mitigating complex cyber threats in real time. As generative AI continues to improve, ensuring their security will be paramount for sensitive data protection, retention of user trust, and wide adoption. The proposed system lays the foundation for further advances in AI security by offering a holistic solution to one of the most pertinent challenges in the AI domain today.

FUTURE RESEARCH DIRECTIONS

While the proposed security system in itself is a great advancement into the security vulnerabilities of generative AI systems, there are identified key areas where future areas of research can enhance/enlarge the capabilities of the generic framework. As generative-AI technologies evolve and emerge into newer applications, the security exposures will be further complicated, hence posing continuous demands for innovation in effective AI security.

➢ *Improving Adversarial Defence Mechanisms*

While the current system has already applied some methods, like DeepFool and the Joint Energy-based Model, in detecting adversarial input, further research can be done to explore newer schemes that offer better defence. These may include:

- **Generative Adversarial Network-based defence systems:** The power of GANs can be used to generate automatically the counterexamples to the adversarial inputs, which may increase the robustness of AI systems.
- **Robust Optimization:** Investigating optimization strategies in order to enhance model resilience against adversarial perturbation without any degradation of performance is further needed for possible improvement.
- **Transfer Learning for Adversarial Detection:** Adversarial attacks keep evolving, and it would be interesting to apply transfer learning techniques in adapting models that already exist to new types of attacks and enhance the system's adaptability to emerging threats.

➢ *Enhancing Token Security*

While JWT authentication plays a very important role in securing access, further research into improving the security of tokens will contribute much to the integrity of systems. The possible future directions might be:

- **Quantum-Resistant JWT:** With the development of quantum computing, there is a need to develop quantum-resistant algorithms in JWT for long-term security.
- **Dynamic Token Systems:** Instead of the research being done on the static token, dynamic tokens would be employed, which periodically change or are based on more advanced cryptographic mechanisms that reduce the possibility of token theft or misuse.
- **Token-Based Behaviour Analysis:** While more integration is in the scope of behavioural biometrics analysis, future research may be focused on deeper analysis, not only of tokens themselves but also on the context in which this token is used, considering such aspects as the pattern of typing or the orientation of the device, user-specific characteristic features.

➢ *Real-Time Threat Detection and Response*

This can be further extended to the existing system for an improved real-time threat mitigation by integrating other AI techniques into the platform and enhancing detection accuracy. Further research may focus on:

- **AI-Powered Automated Incident Response:** A vision for a fully automated intelligent incident response system is the ability of the system not just to detect threats but to trigger on its own and automatically execute the appropriate responses—such as mitigating impact, updating models, and notifying in real-time.
- **Hybrid Security Systems:** Integrating different models of AI into a hybrid system can improve threat detection. For instance, it could be able to merge models utilizing anomaly detection techniques with supervised learning methods or reinforcement learning to allow the system to learn from the evolution in the nature of cyber threats.
- **Edge AI Security:** Most of the AI systems are considering the edge computing environment. Keeping this in mind, the lightweight real-time detection system operative on edge devices will assure generative AI security—one of the important future research areas.

➢ *Integration with AI Governance Frameworks*

As the adoption of AI systems continues to expand, it is more important than ever that such systems are not only secure but also transparent, accountable, and ethical. Future work should aim to:

- **AI Explainability and Transparency:** Building explainable AI frameworks into the security system will, for end-users and administrators, make meaningful what decisions are made and for what reason, creating a need and desire for accountability and trust.
- **Ethics and Privacy in AI:** Future research needs to be done in order for AI models, especially generative AI, to align with ethics guidelines and privacy regulations, such as GDPR or CCPA. This includes, but is not limited to, the assurance that generative AI does not create biased, harmful, or misleading content, while these systems themselves are capable of protecting user privacy.
- **Regulatory Compliance:** Future research could use the case of SASE to investigate issues such as how security frameworks must be revised in light of changing regulations and compliance associated with AI across different geographies.

➢ *Cross-Domain Security Solutions*

Generative AI systems often apply to a wide array of domains, including but not limited to healthcare, finance, media, and e-commerce, each domain with its unique set of security requirements. Cross-domain security solutions that can be adaptable in various industries are needed in order for the mass-wide adoption of secure generative AI. Areas of research include:

- **Domain-Specific Threat Models:** Development of threat models for selected sectors, such as healthcare or financial services, with regard to the specific vulnerabilities that this type of AI may turn out to have in these contexts.
- **Federated Learning for Security:** In a setting where data privacy is paramount, federated learning will have models trained on several decentralized devices or servers while the data remains local. Future research could look into how federated learning can be securely deployed with SASE to maintain privacy while having robust security.

➢ *Enhancing Scalability and Performance*

With large, complex generative AI systems now common and deployed widely, the capability of the security system to scale effectively will be a key factor. Future research activities may be performed in:

- **Security in a Distributed Architecture:** This is for the study of distributed architecture for the implementation of SASE and ZTN in extra-large, very large, and multi-cloud settings and to make the mechanism of security scale across variously and diversely geographically dispersed systems efficiently.

- **Low-Latency Threat Detection:** Investigations into low-latency machine learning algorithms, optimized for high-throughput environments, may finally bring performance improvements in real-time applications with respect to anomaly detection and threat mitigation.
- **Resource-Efficient Security Algorithms:** Lightweight and resource-efficient development of AI models running on resource-constrained environments like edge devices without compromising the security of the algorithm will be one of the major research areas.

➢ *Collaborative Security Solutions*

As generative AI systems will be increasingly integrated with other technologies such as IoT, blockchain, and cloud computing, there will be an increased demand for cross-system collaborative security frameworks. Valuable research areas may involve:

- **Interdisciplinary AI Security:** Collaborating with fields such as IoT security, blockchain technology, and cloud computing security could provide insights into new ways to address vulnerabilities that arise from the convergence of these technologies.
- **Network for Threat Intelligence Sharing:** Creating a global or sectoral network to share threat intelligence would hopefully make the rapid identification of, and response to, newly developed threats in the generative AI ecosystem possible.

The future of securing generative AI systems depends on continued evolution in adaptive, scalable, intelligent security frameworks integrating real-time anomaly detection, advanced adversarial defences, and cross-domain solutions. As generative AI applications continue to grow in complexity and adoption, future research will need to concentrate on emerging threats, system performance, and evolving ethical and regulatory compliance. It is in addressing these challenges that future systems are able to keep the integrity and trust of generative AI systems while allowing their responsible and safe deployment into real-world applications.

ACKNOWLEDGEMENTS

Above all, let us express our deep appreciation to those who, in various ways, have supported us throughout this research.

We would like to take this opportunity to express our heartfelt thanks to our guide, Mrs. V. Padmapriya, Assistant Professor in the Department of Information Technology, for her highly valuable guidance, expertise, and continued support throughout the development of this paper. Her extremely resourceful suggestions and valuable feedback have immensely shaped this research.

We would also like to thank the Department of Information Technology at Sri Manakula Vinayagar Engineering College for the resources and a very good academic environment that enabled us to do this work.

We first wish to express our profound gratitude to our families, who were patient, encouraging, and understanding during this project. They are indispensable cornerstones in the road to success.

Lastly, words of thanks go to researchers and authors whose works have been referenced in this paper. Their works on Generative AI, cybersecurity, and SASE have been very foundational to the concepts and solutions represented here.

REFERENCES

[1]. M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," Department of Computer Science, Tennessee Tech University, Cookeville, TN, USA, 2023. http://dx.doi.org/10.48550/arXiv.2307.00691

[2]. L. Liu, C. Huang, D. Zhu, D. Liu, J. Ni, and X. S. Shen, "Secure and Distributed Access Control for Dynamic Pervasive Edge Computing Services," in *GLOBECOM 2022 - IEEE Global Communications Conference*, Rio de Janeiro, Brazil, 2022, pp. 5487-5492. doi: 10.1109/GLOBECOM48099.2022.10000715.

[3]. N. Din, M. Waheed, M. Zareei, and F. Alanazi, "An Improved Identity-Based Generalized Signcryption Scheme for Secure Multi-Access Edge Computing Empowered Flying Ad Hoc Networks," *IEEE Access*, vol. 9, pp. 120704-120714, 2021. doi: 10.1109/ACCESS.2021.3108130.

[4]. Y. Xia, J. Zhang, and K. L. Man, "A Survey on Handover Authentication for Multi-Access Edge Computing: Classification, Analysis, and Future Directions," in *International Conference on Platform Technology and Service (PlatCon)*, Busan, Korea Republic, 2023, pp. 79-84. doi: 10.1109/PlatCon60102.2023.10255209.

[5]. S. A. Wright, A. Sathyagiri, and R. Tayal, "Machine Learning and the Secure Access Service Edge," in *Congress in Computer Science, Computer Engineering & Applied Computing (CSCE)*, Las Vegas, NV, USA, 2023, pp. 2251-2258. doi: 10.1109/CSCE60160.2023.00367.

[6]. J. Liu et al., "SDSS: Secure Data Sharing Scheme for Edge Enabled IoV Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 11, pp. 12038-12049, Nov. 2023. doi: 10.1109/TITS.2023.3287643.

[7]. W. Jin, R. Xu, T. You, Y.-G. Hong, and D. Kim, "Secure Edge Computing Management Based on Independent Microservices Providers for Gateway-Centric IoT Networks," *IEEE Access*, vol. 8, pp. 187975-187990, 2020. doi: 10.1109/ACCESS.2020.3030297.

[8]. S. Saha, B. Bera, A. K. Das, N. Kumar, S. H. Islam, and Y. Park, "Private Blockchain Envisioned Access Control System for Securing Industrial IoT-Based Pervasive Edge Computing," *IEEE Access*, vol. 11, pp. 130206-130229, 2023. doi: 10.1109/ACCESS.2023.3333441.

[9]. L. Yuan et al., "CoopEdge+: Enabling Decentralized Secure and Cooperative Multi-Access Edge Computing Based on Blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 3, pp. 894-908, Mar. 2023. doi: 10.1109/TPDS.2022.3231296.

[10]. P. Ranaweera, V. N. Imrith, M. Liyanag, and A. D. Jurcut, "Security as a Service Platform Leveraging Multi-Access Edge Computing Infrastructure Provisions," in *IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6. doi: 10.1109/ICC40277.2020.9148660.

[11]. M. Kim et al., "A Secure Batch Authentication Scheme for Multi-access Edge Computing in 5G-Enabled Intelligent Transportation System," *IEEE Access*, vol. 10, pp. 96224-96238, 2022. doi: 10.1109/ACCESS.2022.3205001.

[12]. Q. Huang, C. Wang, and L. Chen, "Secure and Fine-Grained Flow Control for Subscription-Based Data Services in Cloud-Edge Computing," *IEEE Transactions on Services Computing*, vol. 16, no. 3, pp. 2165-2177, May-June 2023. doi: 10.1109/TSC.2022.3203378.

[13]. Y. Guan, S. Guo, P. Li, and Y. Yang, "Secure and Verifiable Data Access Control Scheme With Policy Update and Computation Outsourcing for Edge Computing," in *IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS)*, Hong Kong, 2020, pp. 398-405. doi: 10.1109/ICPADS51040.2020.00060.

[14]. J. P. Queralta, L. Qingqing, Z. Zou, and T. Westerlund, "Enhancing Autonomy with Blockchain and Multi-Access Edge Computing in Distributed Robotic Systems," in *Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, Paris, France, 2020, pp. 180-187. doi: 10.1109/FMEC49853.2020.9144809.

[15]. Khan, A. Ghani, S. M. Saqlain, M. U. Ashraf, A. Alzahrani, and D.-H. Kim, "Secure Medical Data Against Unauthorized Access Using Decoy Technology in Distributed Edge Computing Networks," *IEEE Access*, vol. 11, pp. 144560-144573, 2023. doi: 10.1109/ACCESS.2023.3344168.

[16]. X. Zhou, D. He, J. Ning, M. Luo, and X. Huang, "AADEC: Anonymous and Auditable Distributed Access Control for Edge Computing Services," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 290-303, 2023. doi: https://doi.org/10.1109/TMC.2023.332330

[17]. Nimeshkumar Patel, "Secure Access Service Edge (Sase): Evaluating The Impact Of Converged Network Security Architectures In Cloud Computing," *© 2024 JETIR March 2024, Volume 11, Issue 3 www.jetir.org(ISSN-2349-5162)*

[18]. Sivakameni Indran, Najwa Hayaati Mohd Alwi, "Systematic Literature Review on Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) Implementation to Ensure Secure Access," *Journal of Advanced Research in Applied Sciences and Engineering Technology56, Issue 2(2026) 182-19*, https://doi.org/10.37934/araset.56.2.182195

[19]. Taurai Hungwe and Hein Venter, "An AI Model for Digital Forensic Readiness in the Cloud Using Secure Access Service Edge" *Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024 https://doi.org/10.34190/iccws.19.1.2132 .*

[20]. Zohaib S.M., Sajjad, S.M., Iqbal, Z., Yousaf, M., Haseeb, M., Muhammad, Z "Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work," Information 2024, 15, 734. https://doi.org/10.3390/info15110734