Vol: 3, Issue: 1, 2025
Pages:28-43
Received: 26 March 2025
Accepted: 9 May 2025

CURRENT TRENDS IN COMPUTING
Research Article
DOI: 10.71074/CTC.1666265

ENSURING VIDEO CONFERENCING APPLICATIONS SECURITY: PRIVACY, CHALLENGES AND RISKS

İSA AVCI[1]*, ELIF YILDIRIM[1] AND ELIF SARE AKDAĞ[1]

[1] *Computer Engineering Department, Karabük University, 78050, Karabük, Türkiye*

ABSTRACT. **With the COVID-19 pandemic, video conferencing applications have played a critical role in both individual and corporate communication. However, the widespread adoption of these platforms has brought significant privacy and security threats. This study analyzes popular video conferencing applications (Zoom, Microsoft Teams, Google Meet, Skype, Cisco Webex, GoToMeeting, and TeamLink) from a security and privacy perspective, detailing aspects such as authentication mechanisms, data encryption methods, authorization policies, and security vulnerabilities. The findings reveal that end-to-end encryption support, authentication mechanisms, and security protocols vary across platforms. The results emphasize that selecting a platform according to security needs should be based on encryption algorithms, authentication methods, and security certifications.**

1. INTRODUCTION

The COVID-19 pandemic significantly reshaped communication practices across the globe, forcing a transition from in-person meetings to virtual environments through the adoption of video conferencing platforms [1]. What initially began as an emergency response has since evolved into a permanent shift in how people connect, collaborate, and conduct business [2]. Platforms such as Zoom, Microsoft Teams, and Google Meet are no longer situational tools; they are now deeply integrated into remote work systems, online education, e-health services, and international collaboration frameworks. This widespread use has amplified concerns regarding the security and privacy of user data, calling for robust protection mechanisms [3], [4]. A variety of reports and academic studies have highlighted critical vulnerabilities in popular video conferencing systems. Notably, the South African Parliament's Zoom session was hijacked after access credentials were publicly posted on Twitter [5], and the European Union Defense Ministers' confidential meeting was breached by a journalist who inferred the access code from a shared image [6]. Similar incidents have been reported in the education sector, where unauthorized individuals have disrupted virtual classrooms by sharing inappropriate content, further emphasizing the need for improved safeguards [7].

E-mail address: isaavcı@karabuk.edu.tr (*), elifyildirim@karabuk.edu.tr, 2110206070@ogrenci.karabuk.edu.tr.
Key words and phrases. Video Conferencing Security, Privacy Threats, Secure Communication Technologies.

FIGURE 1. **Tweet Containing the Zoom Meeting Access Information of the South African Parliament on May 7, 2020 [5].**

Beyond such direct intrusions, researchers have demonstrated how personal data can be extracted from publicly available screenshots, video frames, and visual metadata. In one study, over 15,700 video collage images and more than 142,000 face images were analyzed using facial recognition and optical character recognition (OCR) methods to identify users' names, demographics, and social media profiles [8]. These findings illustrate the ease with which individuals can be profiled, especially vulnerable groups such as children and elderly users, posing significant risks in both digital and real-world contexts.

Moreover, the evolution of video conferencing security policies in response to growing concerns has significantly altered the landscape. In the early stages of the pandemic, many platforms lacked advanced encryption, access control, or meeting moderation features [9]. Public pressure and documented incidents, however, compelled service providers to enhance their infrastructures. For instance, Zoom initially restricted end-to-end encryption (E2EE) to paid users, but later made it universally available after criticism. Similarly, platforms such as Microsoft Teams and Google Meet introduced waiting rooms, participant verification, and host management tools to better safeguard sessions. These developments highlight that assessing the current state of platform security must go beyond static feature analysis and incorporate the trajectory of policy changes and user feedback.

While prior literature has addressed technical aspects of conferencing systems, including encryption schemes and threat categories, it often lacks platform-specific comparisons and incident-based evaluations. For instance, the comprehensive survey by Balasubramanian et al. [10] offers a technical overview of conferencing architectures and protocols but does not extend to real-world event analysis or comparative evaluation of individual platforms. This paper seeks to bridge that gap by combining theoretical foundations with practical security insights.

The aim of this study is to conduct a comparative analysis of widely used video conferencing platforms—Zoom, Microsoft Teams, Google Meet, Skype, Cisco Webex, GoToMeeting, and TeamLink—focusing on their security architectures, known vulnerabilities, and privacy models. By leveraging official documentation, scholarly literature, and real-world breach reports, the study provides an integrated evaluation that reflects both technical robustness and practical effectiveness. In doing so, the work offers a distinctive contribution that not only enhances academic understanding but also guides policymakers, IT professionals, and users in selecting secure video conferencing solutions.

2. Related Work

In recent years, numerous academic studies have addressed the security and privacy concerns of video conferencing platforms. Karim and Ali [11] conducted a comparative cybersecurity analysis of Zoom, Microsoft Teams, and Google Meet, concluding that Google Meet was the most secure against cyberattacks, followed by Teams, and lastly Zoom. Gauthier and Husain [12] performed dynamic security testing on the same platforms by analyzing network traffic during simulated meetings. Their findings revealed that none of the three platforms offered true end-to-end encryption (E2EE); while data transmission was encrypted, the service providers retained access to the content. Furthermore, suspicious background activity such as unexplained TCP and DNS connections was observed, raising potential concerns over transparency and privacy.

Encryption models vary significantly across platforms. Zoom faced considerable criticism early in the pandemic due to its weak cryptographic design. A report by Citizen Lab revealed that Zoom employed a single AES-128 ECB key for all participants in a meeting and that encryption keys were occasionally routed through servers located in China [13]. Moreover, Zoom was found to have misrepresented its encryption claims, falsely stating the use of AES-256 E2EE. This issue was formally addressed by the U.S. Federal Trade Commission [14], and several organizations including SpaceX and the New York City Department of Education banned Zoom at the time. Zoom later redesigned its security infrastructure and rolled out E2EE to all users. Microsoft Teams introduced E2EE for one-on-one calls, while Cisco Webex had already implemented it earlier. In contrast, Google Meet still does not support full E2EE for group meetings and continues to decrypt data on its servers, relying only on transport-layer encryption [15].

Threat modeling approaches have also been employed in assessing the security of video conferencing systems. Hasan et al. [16] applied the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to categorize potential attacks on conferencing infrastructures. Their analysis included impersonation, content tampering, unauthorized access to call data, DoS attacks, and privilege escalation. They also addressed physical attacks and brute-force vulnerabilities and proposed mitigation strategies such as hardened encryption, secure authentication, server-side logging, and regular patching.

User behavior and organizational policies also play a critical role in security outcomes. Dassel and Klein [17] found that institutions generally responded to Zoom's early security incidents in three distinct ways: banning the platform outright, applying restrictions and custom security policies, or continuing usage with minimal changes. Many breaches have stemmed from human errors such as weak passwords,

sharing meeting links publicly, or failing to update software. Zoom's now-removed "attention tracking" feature also drew significant criticism and was discontinued due to privacy concerns [18]. These examples demonstrate that technical solutions must be complemented by user awareness, institutional guidelines, and responsive design choices that adapt to privacy expectations.

While the existing literature presents a broad landscape on conferencing security, most studies either focus exclusively on technical architectures or isolate individual incidents. Many fail to connect platform-level vulnerabilities with real-world user behavior, threat modeling, and evolving platform policies. This study aims to fill that gap by providing a multi-layered, comparative analysis that incorporates official documentation, real-world breach reports, encryption evolution, and socio-technical aspects. By doing so, it offers a holistic framework that bridges theoretical understanding and practical application in the domain of video conferencing security.

3. Materials and Methods

This study adopts a document-based qualitative research methodology to evaluate and compare the security and privacy characteristics of seven prominent video conferencing platforms: Zoom, Microsoft Teams, Google Meet, Cisco Webex, Skype, GoToMeeting, and TeamLink. Rather than employing empirical experiments or user-based field surveys, the research relies on the systematic review of publicly accessible data from a wide range of credible sources. These include official platform documentation, technical whitepapers, academic studies on video conferencing security models, cybersecurity reports from independent research firms, public vulnerability databases such as CVE, news reports of verified security incidents, regulatory advisories issued by entities like CERT-In and ENISA, and platform-specific transparency and support portals.

To ensure consistency in analysis and comparability across platforms, the evaluation framework was designed around six interrelated security domains, each of which corresponds to a dedicated subsection in the Findings section. These include the encryption methods and transmission protocols employed for securing communication, the authentication procedures and access control mechanisms in place, adherence to international standards and compliance with privacy and security regulations, platform-level functionalities that may influence the security landscape, previously reported security incidents, and the robustness of incident response and auditing mechanisms implemented by vendors.

Each platform was examined using the same set of thematic lenses, allowing for a structured yet flexible assessment of their security postures. All findings were corroborated through multiple sources wherever possible to ensure validity and minimize the influence of vendor bias. Comparative analysis was further supported by two summary tables designed to highlight both core functional capabilities and specific security and privacy-related attributes.

It should be noted that this study is limited to secondary data available up to early 2025 and does not include active vulnerability testing or access to proprietary enterprise security configurations. These limitations are acknowledged in the conclusion section, and recommendations for future empirical validation are also provided therein.

4. Findings

4.1. **Overview of Online Video Conferencing Applications.**

Online video conferencing platforms have become essential tools in modern communication, extending far beyond basic audio and video transmission. These systems now include functionalities such as screen sharing, virtual background customization, integrated chat, file sharing, and webinar hosting, enabling real-time collaboration across diverse user groups. However, their widespread and growing adoption—particularly in remote work, online education, and global organizational workflows—has brought forth critical concerns related to information security and user privacy.

To understand the security posture of these platforms, this section systematically analyzes the features, security mechanisms, and documented vulnerabilities of several widely-used video conferencing tools. Each platform is assessed based on core attributes such as encryption protocols, authentication mechanisms, compliance with data protection regulations, incident history, and general usability. This comparative evaluation aims to highlight both strengths and weaknesses, providing insight into how security and privacy considerations are implemented in practice. Recommendations are also proposed to mitigate common threats and ensure more secure online meeting environments.

Figure 2 offers a visual summary of the seven video conferencing applications included in this study: Zoom, Microsoft Teams, TeamLink, Google Meet, Skype, Cisco Webex, and GoToMeeting.

Figure 2. **Visual summary of the video conferencing applications analyzed.**

4.2. **Data Transmission and Encryption.**

Secure data transmission and encryption form the backbone of confidentiality in video conferencing applications. While all the platforms analyzed in this study implement some form of encryption, the strategies they employ and the depth of their protection mechanisms vary significantly.

Zoom utilizes AES-256-GCM encryption across all communication streams, offering session-based encryption keys and optional End-to-End Encryption (E2EE) to defend against external breaches [19]. Microsoft Teams ensures data protection both in transit and at rest, with E2EE available for VoIP calls through its Premium version, providing robust integration with Microsoft's enterprise identity services [20]. TeamLink, built on WebRTC standards, employs DTLS, TLS, and SRTP for signaling and media encryption, and notably distinguishes itself by not storing user data on its servers—effectively minimizing post-session exposure risks [21].

Google Meet combines layered encryption protocols such as DTLS and SRTP for real-time data security and uses AES-CTR 256 to encrypt content. However, since the platform applies the Signal Protocol for metadata and decrypts media on Google's servers before storage, its E2EE model remains limited in scope [22]. Skype supports AES-256 encryption for peer-to-peer communications, yet calls routed through the Public Switched Telephone Network (PSTN) are left unencrypted, and post-delivery media files are not protected—undermining comprehensive confidentiality protections [23], [24].

Cisco Webex provides some of the strongest security implementations among the platforms examined. It applies TLS 1.2 and AES-256 for data and media encryption, features a Zero Trust Security model with support for E2EE, and enables on-premises processing through Video Mesh nodes. Webex also encrypts meeting recordings and transcripts using AES-256-GCM and maintains a security infrastructure certified by standards such as SOC 2 and ISO 27001 [25], [26].

GoToMeeting, on the other hand, employs AES-128 encryption and TLS protocols for communication security [27]. While this setup protects data in transit, it is generally considered less secure than AES-256. The platform implements HMAC-SHA-1 and HMAC-SHA-2 for message integrity and signs all client software digitally to prevent tampering [28]. However, it lacks support for full E2EE, meaning that meeting content remains accessible on GoTo's servers. Additionally, the storage of encrypted recordings on AWS S3—although protected—does not fully eliminate server-side access risks. The absence of a Zero Trust architecture or isolated key storage mechanisms makes it less resilient against advanced threats [29], [30].

In summary, Cisco Webex and Zoom stand out with their comprehensive encryption practices and end-to-end data protection. Skype, despite using strong encryption, falls short due to inconsistencies in PSTN call protection. Google Meet and TeamLink offer solid session-level security, while Microsoft Teams balances encryption with scalable enterprise integration. GoToMeeting provides foundational encryption measures, but its reliance on older standards and lack of E2EE places it behind the industry leaders.

4.3. **Authentication and Access Control Mechanisms.**

Authentication and access control are critical components in maintaining the integrity of virtual meeting environments by regulating participant entry, preventing unauthorized access, and enforcing role-based permissions. Although all the examined platforms provide some form of identity verification, their methodologies vary in complexity and effectiveness.

Zoom implements a comprehensive authentication framework, supporting password protection, domain-based access restrictions, Waiting Rooms, SAML and OAuth-based login protocols, and Two-Factor Authentication (2FA), allowing both user-centric and administrator-level control over session access [31]. Microsoft Teams leverages its deep integration with Azure Active Directory and Microsoft 365, providing enterprise-class access management through Single Sign-On (SSO), Multi-Factor Authentication (MFA), and conditional access policies that enable automated and scalable security enforcement [32].

TeamLink offers relatively basic security features, including password-based access control and user-defined meeting restrictions. While it is compatible with Data Loss Prevention (DLP) tools, it lacks support for identity federation protocols such as SSO or OAuth, which limits its appeal in enterprise settings [33]. In contrast, Google Meet requires users to sign in with a Google account and includes Two-Step Verification (2SV), knock-to-join mechanisms, and real-time role-based access management within meetings. It also offers high-assurance protections for sensitive user groups through the Advanced Protection Program (APP) [34].

Skype relies on standard Microsoft account credentials and provides encryption for login data but lacks advanced meeting access tools such as Waiting Rooms, SSO, or dynamic session-based authentication. Its security framework, therefore, remains limited in comparison to modern enterprise needs [23], [24].

Cisco Webex emerges as a leader in this category with its robust authentication model. It integrates with widely-used identity providers like Azure AD, Okta, and Microsoft Active Directory via SSO and applies Role-Based Access Control (RBAC) throughout the platform. Lobby Controls further restrict unauthorized access by requiring authentication prior to joining meetings. Webex also supports multifactor authentication and allows administrators to enforce device and location-specific access policies using its centralized Control Hub interface [26].

GoToMeeting, while implementing basic protections such as password-secured meeting access and TLS-encrypted login, lacks advanced authentication models. It does not currently enforce MFA by default and does not support federated identity systems like OAuth or SSO. This reliance on user discretion for link sharing and account security weakens its administrative access governance. Moreover, the security incident in late 2022, which exposed some MFA configurations across GoTo's ecosystem, highlights the need for improved centralized authentication and identity management practices [27], [28], [29].

Overall, Cisco Webex and Microsoft Teams lead in enterprise-grade authentication and access control, combining technical depth with strong administrative oversight. Zoom also provides flexible user-level protections with widely adopted tools. Google Meet delivers streamlined usability and secure account-level controls. Conversely, TeamLink and Skype remain limited in their offerings, while GoToMeeting, despite covering basic needs, lacks the advanced infrastructure required for secure enterprise deployment.

4.4. **Policy Compliance and Security Certifications.**

Compliance with international security standards and data protection regulations is fundamental for evaluating the reliability, accountability, and legal acceptability of video conferencing platforms, particularly within regulated sectors such as healthcare, education, and public administration. Across the examined platforms, significant differences are observed in certification coverage, transparency, and enforcement capabilities.

Zoom aligns with SOC 2 standards and provides HIPAA-compliant service packages tailored for healthcare institutions. However, its compliance credibility has been questioned due to previous high-profile security incidents, and its adherence to policies is often contingent upon enterprise-level licensing and user-side configuration diligence [19]. Microsoft Teams, on the other hand, demonstrates strong regulatory alignment. It is certified under ISO/IEC 27001, ISO/IEC 27018, HIPAA, GDPR, and both SOC 1 and SOC 2 frameworks. Teams' seamless integration with Microsoft's enterprise ecosystem allows for automated enforcement of policies across users, devices, and shared content, which enhances its compliance robustness [35].

TeamLink claims adherence to enterprise security expectations, supported by DLP integration and a data minimization approach. Nonetheless, the platform does not publicly disclose third-party certifications or audit results, limiting its credibility in environments with strict regulatory requirements [33]. Google Meet benefits from its Google Cloud infrastructure and complies with GDPR, ISO 27001, and HIPAA standards. Google's transparency in publishing vulnerability disclosures and encouraging third-party evaluations through its Vulnerability Reward Program (VRP) strengthens its compliance maturity [34], [36].

Skype does not possess platform-specific certifications and relies primarily on the broader Microsoft Cloud compliance framework. Its lack of HIPAA or SOC-specific certifications renders it unsuitable for use in environments where data sensitivity and regulatory accountability are paramount [23], [24]. Cisco Webex distinguishes itself with a comprehensive range of internationally recognized certifications, including ISO 27001, 27017, 27018, 27701, SOC 2 Type II, SOC 3, and FedRAMP for U.S. federal use. Furthermore, it aligns with GDPR, CCPA, and HIPAA, and offers granular policy controls such as customizable data retention and audit logging to support sector-specific governance requirements [25], [26], [37].

GoToMeeting, although it adopts strong encryption protocols such as AES, TLS, and RSA, provides limited visibility into formal certification frameworks. It does not claim ISO or SOC compliance publicly, and its internal compliance mechanisms were brought into question following a 2022 breach that compromised encrypted backups and certain MFA settings [27], [28], [29].The absence of end-to-end encryption and inadequate key segmentation further weakens its posture in high-compliance environments. These limitations in policy transparency and breach handling constrain GoToMeeting's applicability for use in sectors demanding rigorous regulatory oversight [30].

In conclusion, Cisco Webex and Microsoft Teams emerge as the most robust platforms in terms of compliance infrastructure and certification breadth, suitable for deployment in high-risk or heavily regulated settings. Google Meet upholds a commendable compliance model with proactive risk management strategies. While Zoom offers compliance flexibility, its past security lapses require careful configuration

oversight. Conversely, Skype and TeamLink fall short in formal compliance validation, and GoToMeeting, despite having solid encryption practices, lacks the regulatory transparency and certification depth required for sensitive enterprise use.

4.5. **Platform Functionalities and Additional Features.**

The overall usability and appeal of a video conferencing platform are shaped not only by its security infrastructure but also by its feature set. Advanced functionalities such as real-time transcription, third-party integrations, and collaboration tools play a crucial role in user adoption, particularly within education, enterprise, and healthcare environments.

Zoom is well-known for its feature-rich interface, offering breakout rooms, cloud/local recording, live transcription, screen sharing, virtual backgrounds, and webinar hosting capabilities. Its seamless integration with learning management systems (LMS) and calendar tools has made it a popular choice among universities and remote work teams [19]. Similarly, Microsoft Teams stands out due to its deep integration with the Microsoft 365 ecosystem, enabling features such as threaded chat, real-time document co-authoring, shared calendars, and connections with tools like SharePoint and OneDrive. Its VoIP/PSTN capabilities also enhance its utility for enterprise communication [32], [38].

TeamLink, in contrast, emphasizes performance and simplicity. It provides core functionalities such as screen sharing, recording, and chat, and is valued for its low-latency architecture and compatibility across multiple platforms. While it lacks advanced third-party integration, its lightweight structure makes it suitable for users seeking an efficient and streamlined experience [33]. Google Meet, hosted within the Google Workspace ecosystem, offers a browser-based platform that includes live captions, polls, breakout rooms, and intuitive calendar scheduling. Its minimalist design ensures fast deployment, making it especially useful in educational institutions without dedicated IT infrastructure [34].

Skype, once a leader in internet-based communication, now offers basic features such as audio/video calls, screen sharing, voicemail, SMS messaging, and landline calls. However, its functionality remains limited compared to modern competitors; it does not include tools like breakout rooms or collaborative whiteboards, which reduces its suitability for enterprise or academic contexts [23], [24]. In contrast, Cisco Webex provides one of the most comprehensive feature portfolios in the market. It includes real-time translation, noise cancellation, immersive sharing, interactive polls, and AI-driven tools like Webex Assistant that facilitate note-taking, meeting summaries, and task capture. Additionally, its Control Hub enables centralized IT management, and its integrations with Salesforce, LMS platforms, and even wearable technologies support hybrid workforces and field deployments [39], [40].

GoToMeeting, developed by LogMeIn, delivers a balanced suite of communication and collaboration tools. Its core functionalities include HD video conferencing, screen sharing, chat, and meeting recordings, which can be stored securely in the cloud with support for automatic transcription. The platform's browser-based nature ensures broad accessibility, while its compatibility with firewalls and proxies enhances deployment in diverse network environments. Though it lacks advanced AI features or immersive UI elements like those found in Webex, it remains a dependable solution for small to mid-sized businesses focused on security and simplicity [27], [28].

Taken together, Cisco Webex and Microsoft Teams provide the most advanced and integrated feature ecosystems, making them well-suited for enterprise and government use. Zoom also offers considerable flexibility, particularly in education and webinar settings. Google Meet balances simplicity with effectiveness, whereas TeamLink and GoToMeeting cater to users seeking streamlined, resource-efficient platforms. Skype, though still functional, is now better aligned with personal or informal use cases rather than structured organizational communication.

4.6. **Documented Security Incidents.**

Video conferencing platforms have encountered various security incidents, exposing differences in infrastructure resilience and vendor responsiveness. A comparative review of documented breaches reveals how each provider has handled vulnerabilities over time. Zoom faced widespread scrutiny due to high-profile breaches. Predictable meeting IDs enabled "Zoombombing," and Windows UNC path issues allowed malware distribution via clickable chat links [41]. A 2020 data breach exposed over 500 million user credentials, followed by an 85 million dollar class-action settlement related to unauthorized data sharing with third parties [42]. Further vulnerabilities—such as phishing campaigns, CERT-In advisories, and a macOS privilege escalation flaw—underscored ongoing security challenges [43].

Microsoft Teams, while operating within Microsoft's broader security ecosystem, has also experienced critical issues. An IP address leakage vulnerability on Android devices highlighted risks in data transmission. Additionally, Microsoft disclosed remote code execution flaws that could allow full system compromise if unpatched. These incidents were addressed swiftly via official advisories and updates, reflecting Microsoft's commitment to secure platform maintenance [44].

TeamLink has not been linked to specific publicly disclosed breaches, but potential vulnerabilities stem from weak user-side practices and limited authentication controls. Insecure meeting recordings, misconfigured screen sharing, and outdated encryption algorithms pose theoretical risks of data interception and account compromise. The platform's reliability depends heavily on frequent updates and adherence to modern cryptographic standards.

Google Meet, while backed by Google's robust infrastructure, has also faced criticism regarding past security practices. Prior to 2020, the platform allowed open access via meeting links without mandatory authentication, raising concerns over unauthorized access through leaked or stolen credentials [45]. Although improvements have since been made, phishing attempts using fraudulent invitations and social engineering remain persistent threats. Moreover, Google Meet encrypts data in transit but not end-to-end, meaning meeting content is processed on Google's servers—an approach that some experts view as a potential privacy risk. Users are encouraged to apply two-step verification, moderator tools, and Google's Advanced Protection Program to enhance overall session security [45].

Skype presents a different risk profile, largely centered around web-based infrastructure vulnerabilities. The absence of a valid Content Security Policy (CSP) and misconfigured HTTP headers exposes Skype to Cross-Site Scripting (XSS), Clickjacking, and MIME-based attacks. Weak DNS configurations, such as the lack of DNSSEC and non-enforced HTTPS on subdomains, further increase exposure to domain spoofing and Man-in-the-Middle (MITM) attacks. In addition, reliance on outdated cipher suites and

JavaScript libraries (e.g., jQuery 3.4.1) may render communications more susceptible to cryptographic attacks if not addressed proactively [46].

Cisco Webex has also exhibited several structural security weaknesses. An improperly configured Content Security Policy (CSP) may allow XSS attacks, while its DMARC email policy is insufficiently strict for phishing prevention. Webex lacks DNSSEC and HTTP Strict Transport Security (HSTS) enforcement, making users vulnerable to MITM attacks—especially during first-time connections. Additionally, the use of weak TLS cipher suites increases the risk of encrypted communication compromise [47].

GoToMeeting, although not directly compromised, shares its infrastructure with other GoTo services that were affected in a major 2022–2023 breach. Attackers accessed encrypted backups and some encryption keys for multiple GoTo products, exposing account usernames, hashed passwords, MFA settings, and licensing data [29]. The breach highlighted flaws in access control, encryption key management, and the lack of a Zero Trust Architecture (ZTA) approach. GoToMeeting also lacks end-to-end encryption, which leaves meeting content accessible to servers. Predictable meeting links and weak authentication mechanisms further increase the risk of unauthorized access. Recommendations include enforcing E2EE, mandatory OAuth-based authentication, and MFA across all user accounts [29].

4.7. **Incident Response and Audit Practices.**

Effective incident response and auditing capabilities are critical components of any secure video conferencing platform. These mechanisms ensure timely detection of anomalies, forensic investigation of breaches, and implementation of preventive measures to avoid recurrence. Platforms such as Cisco Webex have demonstrated a mature approach by maintaining a dedicated Product Security Incident Response Team (PSIRT), leveraging internal and third-party audits, and employing threat modeling and static/dynamic testing procedures as part of their Secure Development Lifecycle (SDL) processes [25]. Similarly, Google Meet utilizes machine learning-based anomaly detection systems, regular penetration tests, and a Vulnerability Reward Program (VRP) that engages independent researchers to strengthen the platform's security posture [36]. In contrast, Zoom responded to publicized breaches by implementing employee training programs, notifying users about third-party application access, and committing to stricter privacy controls after a class-action settlement [42]. Microsoft Teams, benefiting from integration with Microsoft's broader security infrastructure, relies on continuous monitoring and automated remediation capabilities within the Microsoft 365 Defender suite [44]. While TeamLink and GoToMeeting lack detailed disclosures about audit practices, the latter faced criticism following a 2023 security breach that revealed weaknesses in its key management and backup segmentation policies [29]. Skype, on the other hand, does not maintain a clear or documented incident response policy and exhibits several misconfigurations such as lack of DNSSEC, improper Content Security Policy (CSP) implementation, and outdated JavaScript libraries, increasing the likelihood of successful exploitation attempts [46].

4.8. **Comparative Summary Tables.**

The following tables provide a concise comparison of the selected video conferencing platforms in terms of functionality and security capabilities. Table 1 outlines the core features that support collaboration and usability across platforms, including meeting support, screen sharing, breakout rooms, and

integration options. Table 2 highlights key security-related aspects such as encryption protocols, authentication mechanisms, compliance with recognized standards, and known vulnerabilities. Together, these summaries complement the detailed platform-specific analyses discussed earlier in this section.

TABLE 1. **Comparison of core functionalities in video conferencing applications**

Platform	Meetings	Screen Sharing	Recording	Breakout Rooms	White/Poll	Calendar	LMS/CRM
Zoom	Yes	Yes	Yes	Yes	Yes	Yes	Yes*
Microsoft Teams	Yes	Yes	Yes	Yes	Yes	Yes	Yes*
Skype	Yes	Yes	Yes	No	No	Yes	Yes
Google Meet	Yes	Yes	Yes*	Yes*	Yes*	Yes	Yes*
Cisco Webex	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TeamLink	Yes	Yes	Yes	No	No	No	No
GoToMeeting	Yes	Yes	Yes	Yes	Yes	Yes	Yes*

(Features available only with certain paid or enterprise editions)*

TABLE 2. **Security and privacy overview of video conferencing tools**

Platform	**Encryption**	**Authorization**	**Compliance**	**Risk**
Zoom	Yes	Yes	Yes	Yes
Microsoft Teams	Yes	Yes	Yes	No
Skype	Yes	Yes	Yes	Yes
Google Meet	Yes	Yes	Yes	No
Cisco Webex	Yes	Yes	Yes	No
TeamLink	Yes	Yes	No	Yes
GoToMeeting	Yes	Yes	Yes	Yes

5. CONCLUSION

This study examined the privacy and security mechanisms of seven widely used video conferencing platforms—Zoom, Microsoft Teams, Google Meet, Cisco Webex, Skype, TeamLink, and GoToMeeting—through a document-based comparative analysis. The increasing integration of video conferencing tools into professional, educational, and governmental environments has made their security and privacy features a critical area of inquiry. While the COVID-19 pandemic catalyzed widespread adoption, the sustained growth in remote work and global digital collaboration continues to highlight the importance of robust and transparent security frameworks.

The primary aim of this study was to systematically evaluate the strengths and weaknesses of each platform with regard to encryption protocols, authentication systems, regulatory compliance, auditability, and past security incidents. By organizing findings under clearly defined thematic dimensions and supplementing them with structured tables, this paper offers a more comprehensive and up-to-date comparative framework than many existing studies in the literature. Unlike prior works that often focus on

a single platform or offer general overviews, this research presents a feature-by-feature security breakdown, integrates historical incident analysis, and synthesizes insights from academic, industrial, and technical sources.

Findings reveal considerable variation in how platforms approach core security principles. For instance, while some services employ strong authentication and encryption schemes, others lack essential protections such as end-to-end encryption or robust patching protocols. Platforms like Zoom and GoToMeeting have experienced notable data breaches, underscoring the need for stricter access control and encryption key management. Meanwhile, services such as Microsoft Teams and Google Meet, though better integrated with enterprise environments, remain susceptible to social engineering, phishing, or structural weaknesses in early versions.

Although this study highlights critical concerns and recommends practical mitigations (e.g., enforcing MFA, segmenting cloud environments, adopting Zero Trust Architecture), it is not without limitations. First, the analysis is limited to publicly available documentation, reported incidents, and literature up to early 2025. Real-world vulnerabilities may evolve faster than academic publications can track. Secondly, while efforts were made to validate incidents across multiple sources, the availability and transparency of platform-specific security disclosures vary significantly. Lastly, the scope is limited to desktop/web conferencing applications; mobile-specific or enterprise deployment-specific security issues were not separately analyzed.

Future research may focus on user-side security behaviors, empirical vulnerability testing, or deeper policy compliance audits under different legal frameworks such as GDPR, HIPAA, and CCPA. Longitudinal studies observing how platforms respond to newly emerging threats could also provide valuable insight into the effectiveness of vendor responses over time. In conclusion, this study contributes a structured, comparative perspective to the growing body of research on video conferencing security. It provides stakeholders—including IT administrators, developers, and policy makers—with a foundational resource to guide platform selection, risk assessment, and secure deployment strategies.

DECLARATIONS

- **Contribution Rate Statement:**
  İsa Avcı: writing-original draft, resources, methodology, conceptualization,
  Elif Yıldırım: writing-original draft, resources, methodology, conceptualization,
  Elif Sare Akdağ: writing-original draft, resources, methodology, conceptualization
- **Conflict of Interest:** The authors have not disclosed any competing interests.
- **Data Availability:** Data sharing is not applicable to this article as no datasets were generated or analyzed.
- **Statement of Support and Acknowledgment:** None.

REFERENCES

[1] Avcı, Akıllı ulaşım sistemlerinde siber saldırılar ve önlemler, Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi 6 (1) (2023) 194–208. doi:10.51513/jitsa.1224909.

[2] Avcı, M. Koca, Cybersecurity attack detection model, using machine learning techniques, Acta Polytechnica Hungarica 20 (7) (2023) 29–44.
[3] UNESCO, Covid-19 educational disruption and response, https://en.unesco.org/covid19/educationresponse, accessed: 10-Feb-2025 (2020).
[4] D. Kagan, G. F. Alpert, M. Fire, Zooming into video conferencing privacy and security threats, arXiv preprint arXiv:2007.01059 1, jul. 2020 (2020).
[5] P. of RSA, Public online zoom meeting details, https://twitter.com/ParliamentofRSA/status/1258289355682123779, accessed: Feb. 25, 2025 (2020).
[6] A. Ötesi, Hollandalı gazeteci ab savunma bakanlarının gizli zoom toplantısına sızdı, https://anlatilaninotesi.com.tr/20201122/hollandali-gazeteci-ab-savunma-bakanlarinin-gizli-zoom-toplantisina-sizdi-1043268675.html, accessed: Feb. 25, 2025 (2020).
[7] A. Ötesi, Bursa'da öğrencilerin uzaktan eğitimine siber sapık engeli, https://anlatilaninotesi.com.tr/20201203/bursada-ogrencilerin-uzaktan-egitimine-siber-sapik-engeli-1043337519.html, accessed: Feb. 25, 2025 (2020).
[8] G. Varghese, Effectiveness of virtual learning with security, Bayan College IJMR 1 (1) (2020).
[9] Avcı, Investigation of cyber-attack methods and measures in smart grids, Sakarya University Journal of Science 25 (4) (2021) 1049–1060. doi:10.16984/saufenbilder.955914.
[10] S. Balasubramanian, M. Dhanushkodi, K. Balasubramanian, A survey on security and privacy issues in video conferencing systems, IEEE Access 9 (2021) 115293–115308. doi:10.1109/ACCESS.2021.3052536.
[11] F. Karim, A. Ali, E-learning virtual meeting applications: A comparative study from a cybersecurity perspective, https://www.researchgate.net/publication/355949578, accessed: 2025 (2021).
[12] N. H. Gauthier, M. I. Husain, Dynamic security analysis of zoom, google meet and microsoft teams, https://www.researchgate.net/publication/350568748, accessed: 2025 (2021).
[13] B. Marczak, J. Scott-Railton, Move fast & roll your own crypto: A quick look at the confidentiality of zoom meetings, https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/, accessed: Apr. 2020 (2020).
[14] F. T. Commission, Zoom video communications, inc., in the matter of, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3167-zoom-video-communications-inc-matter, accessed: Nov. 2020 (2020).
[15] Google, Learn about call & meeting encryption in google meet, https://support.google.com/meet/answer/12387251, accessed: 2023 (2023).
[16] M. Hasan, M. Hasan, M. Hasan, Towards a threat model and security analysis of video conferencing systems, https://www.researchgate.net/publication/349994212, accessed: 2025 (2021).
[17] K. S. Dassel, S. Klein, To zoom or not: Diverging responses to privacy and security risks, Journal of Business ResearchAccessed: 2025 (2023).
[18] D. Kagan, G. F. Alpert, M. Fire, Zooming into video conferencing privacy and security threats, https://arxiv.org/abs/2007.01059, accessed: Jul. 2020 (2020).
[19] Zoom, Security at zoom, https://explore.zoom.us/en/trust/security/, accessed: 18-Feb-2025 (2025).
[20] M. Support, End-to-end encryption in teams, https://support.microsoft.com, accessed: 2025 (2025).
[21] TeamLink, Meeting security, https://www.teamlink.co/faq/index.html#meeting-security, accessed: 20-Feb-2025 (2025).
[22] Google, End-to-end encryption in duo, https://www.gstatic.com/duo/papers/duo_e2ee.pdf, accessed: 23-Feb-2025 (2018).
[23] Microsoft, Does skype use encryption?, https://support.microsoft.com/en-us/skype/skype-encryption-28f5b30b-fcce-493a-9e55-049add6c2d39, accessed: Feb. 24, 2025 (2025).

[24] Microsoft, How long are files and data stored on skype?, https://support.microsoft.com/tr-tr/skype/dosyalar-ve-veriler-skype-ta-ne-kadar-saklan%C4%B1r-22a11965-4c63-45d7-a56c-ee8908f5cdff, accessed: Feb. 24, 2025 (2025).
[25] Cisco, Webex meeting center: A white paper, https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html, accessed: Feb. 24, 2025 (2025).
[26] Cisco, Webex trust center, https://www.cisco.com/c/en/us/about/trust-center/webex.html, accessed: Feb. 24, 2025 (2025).
[27] LogMeIn, Gotomeeting: Web-based online meetings, desktop screen sharing and video conferencing, https://www.gotomeeting.com, accessed: 24-Feb-2025 (2025).
[28] LogMeIn, Privacy policy, https://www.goto.com/company/legal/privacy/us, accessed: 24-Feb-2025 (2025).
[29] P. Srinivasan, Our response to a recent security incident, https://www.goto.com/blog/our-response-to-a-recent-security-incident, accessed: Feb. 25, 2025 (2023).
[30] LogMeIn, Unified communications collaboration security white paper snapshot, https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/UCC_security_white_paper_snapshot_April2020.pdf, accessed: Feb. 25, 2025 (2020).
[31] Zoom, Zoom official website, https://www.zoom.com/, accessed: 18-Feb-2025 (2025).
[32] Microsoft, Microsoft teams- group chat software, https://www.microsoft.com/tr-tr/microsoft-teams/group-chat-software, accessed: 18-Feb-2025 (2025).
[33] TeamLink, Privacy policy, https://www.teamlink.co/privacy.html, accessed: 20-Feb-2025 (2025).
[34] Google, Google meet güvenlik önlemleri, https://support.google.com/meet/answer/9852160?hl=tr&ref_topic=14074547, accessed: Feb. 23, 2025 (2025).
[35] C. Pro, Microsoft teams ne kadar güvenli?, https://cyberartspro.com/microsoft-teams-ne-kadar-guvenli/, accessed: 18-Feb-2025 (2025).
[36] Google, Google meet'te toplantılara katılma, https://support.google.com/meet/answer/12387251?hl=tr&ref_topic=14074547, accessed: Feb. 23, 2025 (2025).
[37] C. T. Portal, Privacy data map — privacy data sheet, https://trustportal.cisco.com/c/r/ctp/trust-portal.html, accessed: Feb. 24, 2025 (2025).
[38] Microsoft, Microsoft teams online call flows, https://learn.microsoft.com/en-us/microsoftteams/microsoft-teams-online-call-flows, accessed: 18-Feb-2025 (2025).
[39] Webex, Webex meetings, https://www.webex.com/suite/meetings.html, accessed: Feb. 24, 2025 (2025).
[40] Webex, Cage match: Competitive highlights from enterprise connect, https://www.webex.com/content/dam/wbx/us/ebook/cage-match-webex-competitive-highlights-from-enterprise-connect_cm-3648.pdf, accessed: Feb. 24, 2025 (2025).
[41] C. S. Alliance, An analysis of the 2020 zoom breach, https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach, accessed: Mar. 13, 2022 (2022).
[42] CNBC, Zoom reaches $85 million settlement over user privacy and hacker 'zoombombing', https://www.cnbc.com/2021/08/01/zoom-reaches-85-million-settlement-over-user-privacy-and-hacker-zoombombing.html, accessed: Aug. 1, 2021 (2021).
[43] T. Guide, Zoom security issues: What's gone wrong and what's been fixed, https://www.tomsguide.com/news/zoom-security-issues, accessed: Jan. 9, 2023 (2023).
[44] M. Support, Microsoft güvenlik danışma belgesi araçlar'daki güvenlik açıkları uzaktan kod yürütülmesine İzin verebilir, https://support.microsoft.com/tr-tr/topic/microsoft-g%C3%BCvenlik-dan%C4%B1%C5%9Fma-belgesi-ara%C3%A7lar-daki-g%C3%BCvenlik-a%C3%A7%C4%B1klar%C4%B1-uzaktan-kod-y%C3%BCr%C3%BCt%C3%BClmesine-izin-verebilir-9e1afef5-9846-0603-b03a-b106a43cb27b, accessed: 18-Şubat-2025 (2021).

[45] Google, Google meet security measures and best practices, https://support.google.com/meet/answer/9852160?hl=en&ref_topic=14074547, accessed: Feb. 24, 2025 (2024).
[46] UpGuard, Skype security report, https://www.upguard.com/security-report/skype, accessed: Feb. 24, 2025 (2025).
[47] UpGuard, Webex security rating, vendor risk report, and data breaches, https://www.upguard.com/security-report/webex, accessed: Feb. 24, 2025 (2025).