A Security Framework for Addressing Privacy Issues in the Zoom Conference System

Samer Atawneh[1*], Ziad Alshammari[2], Mousa AL-Akhras[3] and Bayan Abu Shawar[4]

[1*]College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia.
satawneh@seu.edu.sa, https://orcid.org/0000-0001-7590-7887

[2]College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia.
ziad.shammari@gmail.com, https://orcid.org/0009-0008-4527-6445

[3]King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan.
mousa.akhras@ju.edu.jo, https://orcid.org/0000-0002-2208-372X

[4]College of Engineering, Al Ain University, Abu Dhabi, UAE. bayan.abushawar@aau.ac.ae,
https://orcid.org/0000-0003-3062-4511

Received: November 14, 2023; Accepted: January 06, 2024; Published: February 29, 2024

Abstract

The COVID-19 pandemic had a significant impact on many facets of human behavior. Most significantly, it required significant changes to how daily activities were conducted. The majority of individuals were forced to work and communicate from home due to social distancing, which opened the door for more virtual meetings. Since most organizations started allowing their employees to work from home, the majority of online meeting platforms—like Zoom and Microsoft Teams—have become more and more popular. Online meetings were not only used by businesses but also by educational institutes to carry out online learning, hospitals to conduct meetings and certain surgeries, and many other industries. The online meetings are practical and simple to organize, but their information security is not as high as that of conventional meetings. Security and privacy issues resulted from this. The safety of personal information such as names, contacts, and locations, the security of online recordings since sensitive information was discussed in most meetings, the security of data while it was in transit, and the potential for competitors to intercept your business were among the many security issues that were raised. Zoom, as one of the famous online conference systems, faced many global concerns, such as sharing private information with third parties, exposing users to unauthorized bullying calls, and adopting questionable end-to-end encryption processes. Additionally, companies have had virtual meetings hacked, leading to privacy issues since hackers can obtain data illegally. Therefore, this research proposes a security framework to address the privacy issues in the Zoom system by applying a set of governance and technical controls. The governance controls provide a strategic view of how an organization controls its security while implementing the technical controls avoids privacy issues in online conference systems. The proposed framework implements a set of technical controls such as encryption, auditing, authentication, and role-based access control. The results were promising and significantly addressed Zoom's privacy issues.

Keywords: Zoom, Conference System, Privacy, Governance, Technical Controls.

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 1 (February), pp. 242-265.
DOI: *10.58346/JISIS.2024.I1.016*

*Corresponding author: College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia.

1 Introduction

This research discusses the privacy issues in the Zoom conference system. This section lays a brief background in terms of the privacy of Zoom. Since the pandemic's start in 2019, the usage of online conference software has increased. Conference systems, such as Zoom, are software programs used to conduct online meetings from various platforms. They have played an important role in improving convenience in meetings. Moreover, Zoom is a cloud-based video and audio-conferencing service that allows you to collaborate, communicate, and hold webinars. Zoom meetings may accommodate up to 1,000 video guests and be accessed through HD video and audio from any device (Singh, & Awasthi, 2020). Research shows that various systems offering video conferencing services, such as Zoom, MS Teams, and Google Meet, have reported increased revenue due to increased use. Table 1 illustrates the revenue increases reported by Zoom from 2019 to 2021. However, since technology has improved, so have security threats (Park et al., 2020).

Table 1: Zoom Revenue (Dean, 2021)

Years	**Jan 2019**	**Apr 2019**	**Jul 2019**	**Oct 2019**	**Jan 2020**	**Apr 2020**	**Jul 2020**	**Oct 2020**	**Jan 2021**	**Apr 2021**	**Jul 2021**
Quarterly Revenue in millions $	106	122	146	167	188	328	664	777	882	956	1021

The weak authentication mechanisms in Zoom have allowed intruders to log into online sessions and steal user data. Such privacy concerns have limited the use of Zoom. Additionally, students have collected their data in online learning platforms, which has attracted hackers to steal the collected information. The implementation of the correct application, which is vital, like OAuth 2.0, has been used by many well-known companies like Facebook, Microsoft, Google, etc., which can be utilized in different ways (Singh & Chaudhary, 2022). One of the ways is to ensure confidentiality and privacy in registering the clients' accounts. This will prevent anyone from accessing a user account that is not theirs. An effective protocol must be created and implemented in conjunction with MPFFT and openPMU. These protocols will prevent any remote monitoring of a video conference.

The Common Vulnerabilities and Exposures (CVE) reports detail the most serious security flaws (Figure 1). In 2018, Zoom released a security report that detailed two key CVEs. The CVE-2018-157152 vulnerability demonstrated how malicious actors might take over users' screens and impersonate chat sessions. Other meeting components can be controlled by sending messages and managing other aspects of the meeting. CVE-2020-114433 described how the Windows Zoom IT Installer, which removes files from your computer, works. Before reinstalling Zoom, the files and data could be exploited to erase files that a user is not supposed to be able to remove. Additional Zoom’s program has been identified to have vulnerabilities, and Zoom has been updated. Patches for these vulnerabilities were provided in response (Mahr. et al., 2021).

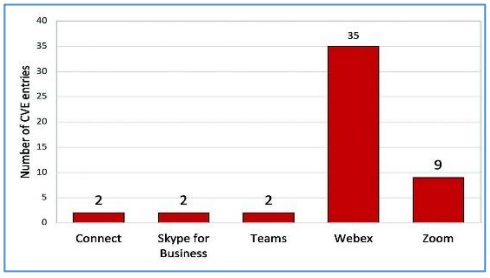

Figure 1: 2020 CVE entries for online meeting platforms (Mahr. et al., 2021)

Data is valuable, and in most instances, systems and programs must provide security assurance on data. However, conference systems, such as Zoom, have privacy issues and concerns that need to be explored. Not many studies exist on privacy issues in Zoom. IT-related crimes and cybercrimes are escalating with the sustainable development of technological aspects within different countries. The newest technology, Zoom, assures users of enormous advantages. Numerous questions and concerns about their security and privacy issues still need to be answered by specialists, and as a result, much research still has to be done in this field. Many privacy and data protection policies still need to be implemented if privacy and security issues are to be managed. However, information technology behemoths like Microsoft, Google, and Cisco are investing heavily in research in the area.

As Zoom has risen in popularity, a new type of video teleconferencing hijacking (also known as "Zoom-bombing") has been reported around the country. Zoom-bombing is the act of interfering with an ongoing phone call. Numerous claims of pornographic and threatening images and disturbing language sessions have been made to the FBI. Meetings have been hijacked in schools, universities, businesses, and government agencies at all levels (Botacin, 2020).

This research contributes to the field of privacy of the Zoom conference system. The research depicts various types of privacy issues that are likely to arise and proposes solutions for reducing and eliminating them over time. The research also aids in the acquisition and identification of various methods and techniques for reducing cyber and IT security-related threats. It also aids in understanding the relationship between the security systems models' availability, integrity, and secrecy. This will assist researchers in gaining vivid thoughts about the notions of cyber security and IT security, allowing them to construct a recommended vision for constructing safe conference tools. The information offered in this research can also be used as a secondary data source in future studies on the same topic.

Therefore, the research aims to evaluate the concept of privacy in the Zoom conference system and proposes a framework to mitigate privacy issues. The contribution of the research objectives is as follows:

- To assess the privacy level in the Zoom conference system.
- To develop a privacy framework to mitigate and eliminate privacy issues in the Zoom conference system.

The rest of the research is organized as follows: Section 2 discusses related work. Section 3 details the proposed framework. Results are discussed in Section 4. Finally, Section 5 concludes the research and presents possibilities for future work.

2 Literature Review

This section will discuss the latest research that handles the Zoom conference system's privacy issues. Zoom is widely used for conferencing and is becoming more well-known all around the world. It offers online chat services through cloud-based peer-to-peer software that is largely used for video conferencing, social interactions, and remote meetings (Susukailo et al., 2020). However, Zoom has serious security and privacy concerns. A major privacy issue is that Zoom has a weak authentication mechanism. This leads to unauthorized people invading Zoom sessions and, thus, denying Zoom users the needed privacy. The ability of an individual to bypass the weak authentication mechanism has created a major security concern. However, this has led to the development of a privacy concern as intruders who bypass the weak authentication mechanism have been known to steal data belonging to Zoom users (Mohanty & Yaqub, 2020).

Goodyear (2019) claimed that security of protection is a legitimate and approachable concern rather than a technical one. Conflicts are being caused by the organizations' ignorance of how their data is being used. The US and European Exchange Commission, which characterizes the seven security assurance criteria, describes the Secure Harbor protection standards system. Some say that customers must be informed about how their information is being collected; a person can also choose not to provide their information if they so choose. Rules approval, freedom of choice, and consent are essential, and disclosure and disclaimers should be employed. On the other hand, attackers disregard these laws and expose victims drastically (Goodyear, 2019). One such unfavorable effect of this problem is that small and medium-sized businesses employing such systems are unaware of the major privacy issues arising from attacks on Zoom conferencing. Such organizations must research while including staff in awareness-raising initiatives for data and privacy protection. Figure 2 shows the likelihood that various types of malicious assaults will occur during organizational, academic, private, and business virtual meetings (Goodyear, 2019).

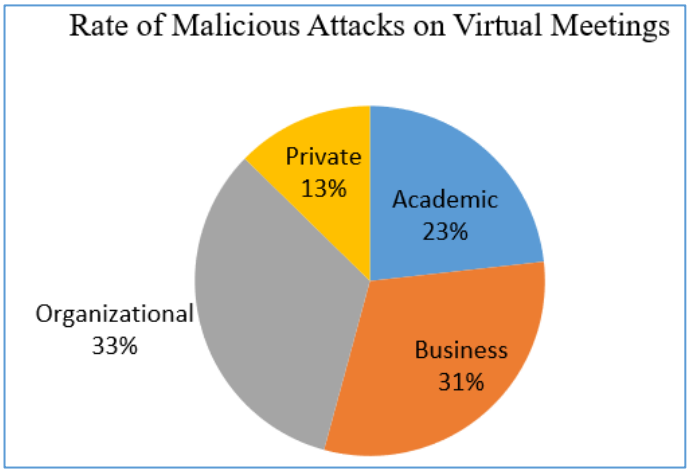

Figure 2: Rate of malicious attacks on virtual meetings (Goodyear, 2019)

Online meetings have created a convenient alternative to face-to-face sessions. The resources acknowledge that most participants are first-time users who had little idea or information about what good security in online meetings would look like. Therefore, a major privacy concern was raised for first-time users who could easily be attacked because their security was weak, and they had little information regarding the security of online meetings (Botha & Furnell, 2021).

Security and privacy issues can come into force in various areas. Figure 3 illustrates the positioning of security issues related to online meetings (Botacin, 2020). As Zoom has risen in popularity, a new type of video teleconferencing hijacking (also known as "Zoom-bombing") has been reported. Zoom-bombing is the act of interfering with an ongoing phone call (Botacin, 2020). Numerous claims of pornographic and threatening images and disturbing language sessions have been made to the FBI. Meetings have been hijacked in schools, universities, businesses, and government agencies at all levels.

In 2020, Zoom provided end-to-end encryption (E2EE) to protect conversations while individuals are in meetings. A thorough security evaluation of the E2EE is conducted in the research, and several attacks were discovered to be more powerful than what Zoom could handle. This was a privacy issue because the study uncovered more powerful attacks that could bypass the E2EE rolled out by Zoom in 2020. Specifically, insiders could impersonate any Zoom user by colluding with meeting participants. This shows the security weaknesses of the E2EE security and why certain users can bypass this security feature (Isobe & Ito, 2021).

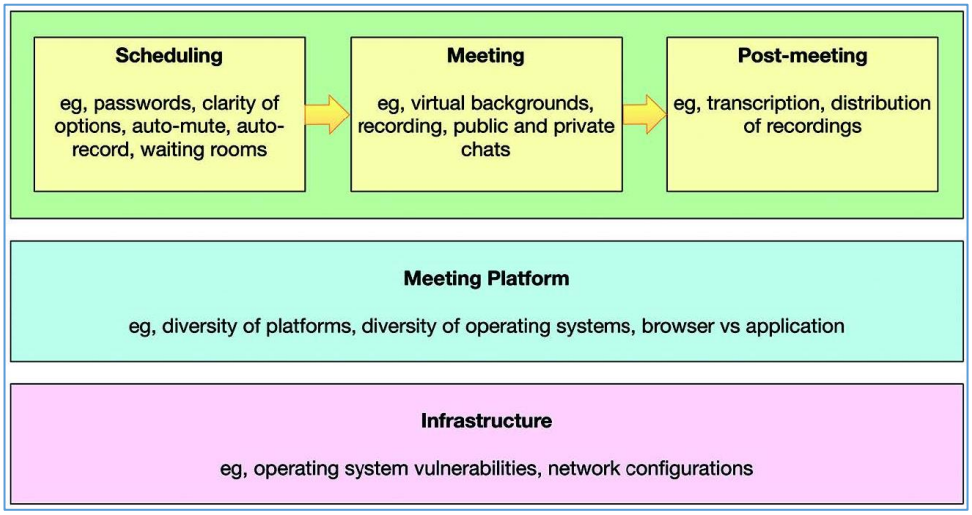

Figure 3: Positioning of security issues related to online meetings (Botacin, 2020)

Aiken (2020) explored the privacy concerns in Zoom as the platform's popularity has increased. Zoom has increased its number of users due to the COVID-19 pandemic since December 2019. The number of virtual meetings moved from 10 million daily to 300 million in four months. However, another security concern has risen with this increase in virtual meetings. Businesses have had virtual meetings hacked, raising privacy issues since hackers can obtain data illegally. Another privacy concern explored in this journal article is the individuals who can access personal information. The data of Zoom users is stored in servers, thus making it vulnerable to attacks.

Global surveys about privacy issues in Zoom were carried out in several countries, such as the United Kingdom, Japan, Mexico, the United States, India, Germany, Singapore, Australia, Brazil, and France. The majority of the population surveyed included individuals who have extensively used the Zoom conference system in frequent video conferences and taken part in regular Zoom video classes, work meetings, holiday gatherings, and even doctor appointments. This is a crucial statistic upon which conclusions can be drawn concerning privacy issues related to the Zoom conference system and its perception by the public in general. In the percentage form, random population samples that were evenly distributed provided their opinion on their take on Zoom privacy issues and their respective choice on whether they can still rely on the Zoom conference system after the termination of the pandemic. Figure 4 illustrates the results of the surveys that were conducted. The percentages reveal the impact of privacy issues that arose from the use of Zoom as a formal conference system for business and educational needs. However, the data analysis also reveals that privacy issues were disregarded in some countries. A strong tradeoff of privacy for relevance and usability is made evident, with the majority opting to continue using the videoconferencing platforms even after their necessity is lessened due to the re-opening of social and working places for normal interactions.

DJEKI et al. (2021) explored how education has been impacted since the pandemic. Schools and universities have relied heavily on online courses to assist in containing the spread of the virus. However, the security vulnerabilities have increased dramatically. Figure 5 illustrates the increase in vulnerabilities over the years in Cisco WebEx Meetings, Skype for Business, and Zoom (DJEKI et al., 2021). In addition, schools and other educational institutes have failed to address security issues brought about by these conference systems. Unfortunately, these online platforms for online classes collect data from students that attract hackers. Figure 6 illustrates the Blackboard LMS Vulnerabilities by Type (DJEKI et al., 2021).

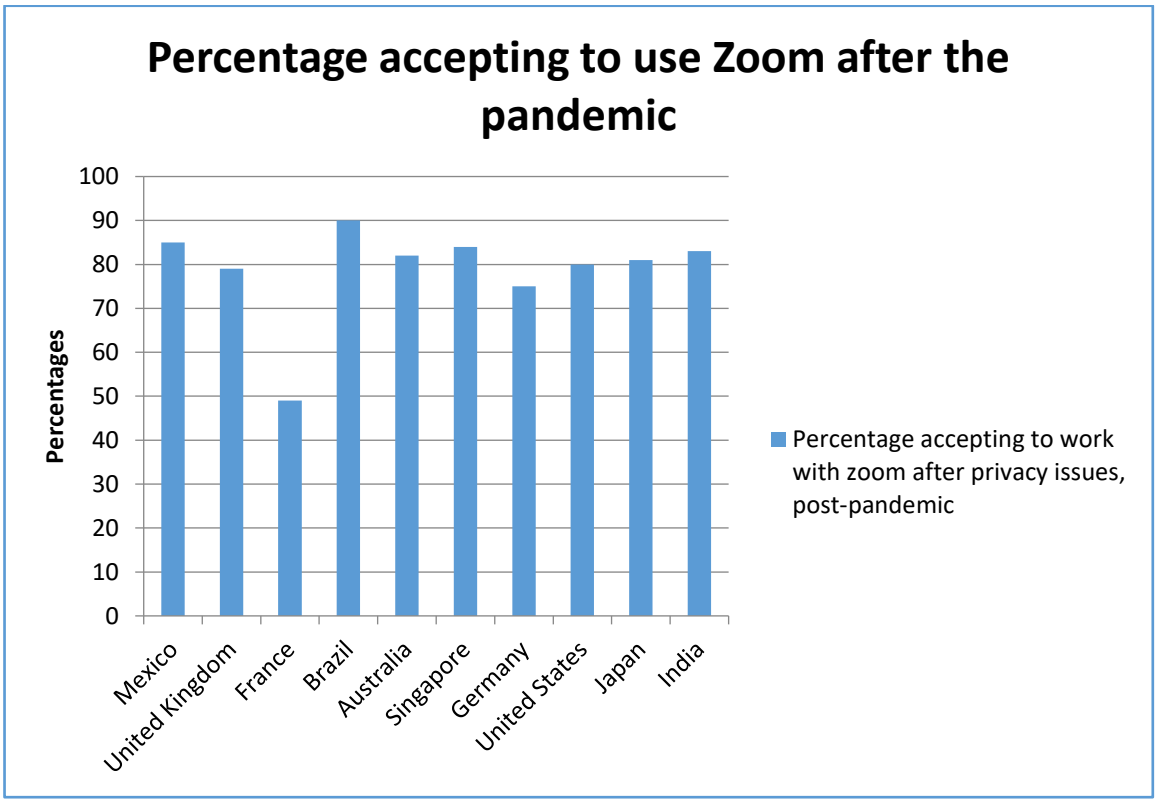

Figure 4: Percentage of accepting to use Zoom after the pandemic in different countries (Zoom, 2021)

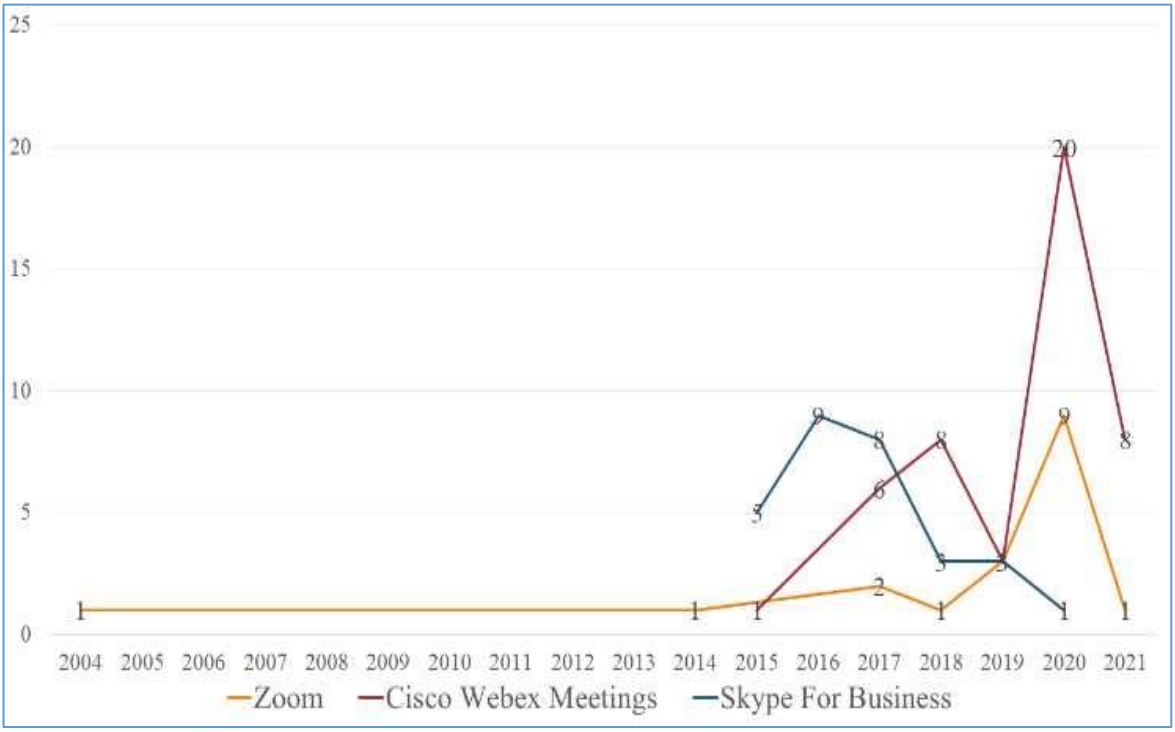

Figure 5: Cisco WebEx meetings, skype for business, and zoom vulnerabilities by years (DJEKI et al., 2021)

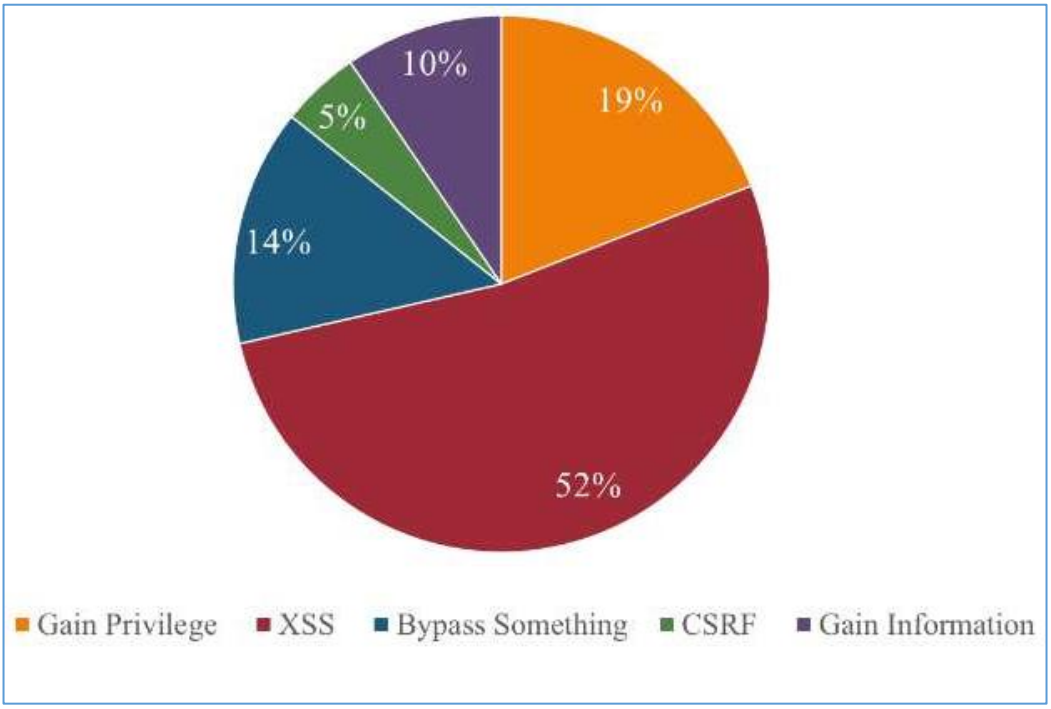

Figure 6: Blackboard LMS Vulnerabilities by Type (DJEKI et al., 2021)

Cobo and Vargas (2022) mentioned that Zoom faced many global concerns, such as sharing private information with third parties, exposing users to unauthorized bullying calls, and adopting questionable end-to-end encryption processes. They added that protecting people from the privacy and security risks associated with using the Zoom system by only offering simple privacy tips will not be enough. Lessons learned from 2020 show that having a deeper understanding of what it means to be online is substantial.

Recently, Kagan et al. (2023) conducted an experimental study to explore Zoom's privacy issues, where private information was extracted from publicly published collage images. The research's results indicate that thousands of publicly available images of meetings can be easily collected, and the people's personal information, such as faces, ages, genders, usernames, and full names, can be extracted. This can easily and vastly jeopardize people's privacy and security in the real world and online. Figure 7 presents a Zoom image collage with detected information and extracted features of gender, age, face, and full name (Kagan et al., 2023).

Several incidents were reported related to security and privacy issues in online meetings:

- 2020 Zoom Breach: During the COVID-19 pandemic, Zoom experienced an unprecedented surge in users, exposing security vulnerabilities. Over 500 million user credentials were compromised, leading to unauthorized access and leakage of confidential information. [https://cloudsecurityalliance.org]
- Microsoft Teams Vulnerabilities: Microsoft Teams faced vulnerabilities related to subdomain takeover and token theft, potentially compromising user accounts. As a result, unauthorized access, data leakage, and account hijacking prompted security enhancements by Microsoft. [https://microsoft.com/security]
- Google Meet Phishing Scams: Google Meet users were targeted by phishing scams aiming to steal credentials by impersonating legitimate communication. This led to potential unauthorized access to Google accounts and sensitive data, leading to heightened security measures.

- Cisco Webex Vulnerabilities: Cisco Webex experienced security vulnerabilities that could allow unauthorized access to meeting data. Potential data breaches expose confidential information, leading to security updates.

Ensuring that security audits are carried out regularly. The sooner security issues are recognized, the better for the teleconferencing business. Business owners should conduct frequent security audits of the platform and watch for any strange activity. During a security assessment, search for weak spots in the systems and propose ideas to improve them. Spend some time teaching employees about cybersecurity threats and what they can do to keep the platform safe. Section 3 presents in detail a proposed privacy framework to handle the privacy issues in the Zoom system.

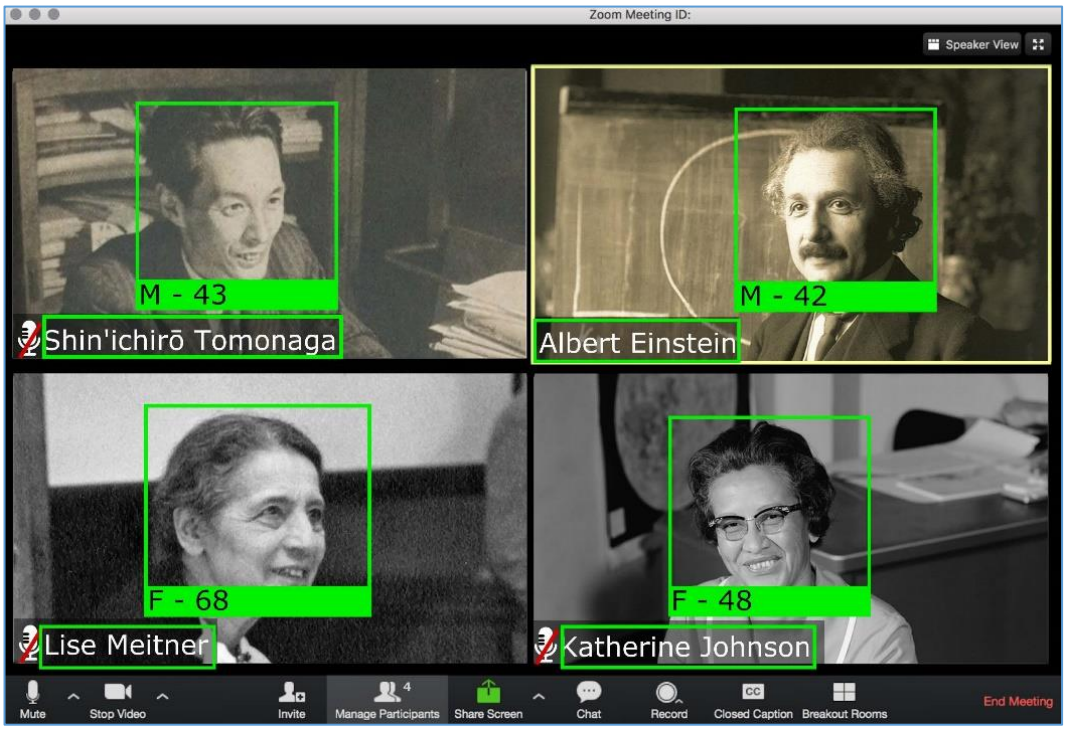

Figure 7: Zoom image with detected information, along with extracted features of gender, age, face, and username (Kagan et al., 2023)

3 Proposed Privacy Framework for Conference Systems

This section presents the proposed privacy framework in detail. Section 3.1 introduces the personally identifiable information (PII) as part of the privacy policy adopted in the proposed framework. Section 3.2 describes conducting the privacy risk assessment as an important step in measuring any conference system's privacy level. Section 3.3 presents the overall methodology for the conducted research. Finally, Section 3.4 shows the implementation of the proposed framework.

Although the idea of a privacy risk is not new to policy, there is currently no advice on how to evaluate this risk. The Organization for the Advancement of Structured Information Standards (OASIS) Privacy Management Reference Model and the International Organization for Standardization (ISO) Privacy Framework both include provisions for privacy risk assessment as part of their frameworks or methodologies. Still, they do not offer instructions on how to carry out a risk assessment.

3.1. Personally Identifiable Information (PII)

Nowadays, personal data usage is a pillar of most recently released IT goods and services. If the right safeguards are not taken, they may, therefore, lead to several privacy violations. Before developing a product that collects or processes personal data, a privacy impact assessment (PIA) should be performed to ensure that such problems are correctly addressed and resolved. A privacy impact assessment is "a process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and examined." Many nations, including Canada, the United States, and the United Kingdom, have led this trend. The National Data Management Office (NDMO) data governance framework by the Saudi Data and AI Authority (SDAIA) and other standards and laws were also implemented in Saudi Arabia by the National Cybersecurity Authority (NCA) (National Data Management Office, 2022).

Due to several information security incidents involving personally identifiable information (PII), which have impacted both people and organizations, we have seen enormous record losses over the past few years. Legal responsibility, identity theft, and recovery expenses are a few examples of different incidents. As a result, companies should develop an international information security standard that offers instructions on how to safeguard their privacy networks and personally identifiable information (PII) to keep up with the growing use of ICTs that handle PII.

Any data used alone or in combination with other sources to specifically identify, contact, or locate an individual is considered PII. First and last names, address data, date and place of birth, and credit card information are a few examples of PII. Personally identifiable information may also comprise highly private information that should only be used in specific circumstances. Their protection is essential since failing to disclose information could have many negative effects. The following are the major justifications for why businesses safeguard their PII:

- To safeguard the privacy of the PII principal.
- To adhere to legal and regulatory standards.
- To engage in corporate responsibility.
- To boost consumer credibility.
- To lessen the frequency of security breaches.

According to the Ponemon Institute survey, "43% of companies have experienced a data breach in the past years, which is up 10% from a year ago." (E. Weise, 2022). Many firms risk running into problems that will cost them a lot of money if they do not take securing PII seriously. A security breach may impact your clients or your clients' clients in addition to harming the information because it might have a cascading effect. Numerous unintended consequences would result from this cycle of destruction for firms, including the imposition of penalties and legal proceedings, disgruntled stakeholders, an exorbitant rise in disaster recovery costs, and ultimately, reputational harm.

In response to ongoing privacy-related issues involving big businesses, little businesses, and well-known people. Recognized organizations like ISO and NIST have made numerous publications on PIAs (Privacy Impact Assessments). The privacy framework architecture is intended to offer a more advanced framework for protecting PII using ICT systems. Through the application of industry best practices, organizations can use these standards to design, install, manage, and maintain ICT systems that will allow the protection of PII. The proposed framework's privacy policy will include PII, which will be covered in Section 3.4.

3.2. Privacy Risk Assessment

An organization can identify and prioritize privacy concerns caused by a system, product, or service by doing a privacy risk assessment. This will enable the organization to make decisions about how to address the risks. Organizations should consider the risk models and risk variables while using different methodologies to conduct privacy risk assessments. The risk elements that need to be evaluated, as well as their correlations, are specified by risk models. An organization should specify which risk variables it will be evaluating and how these elements relate to one another if it is not using a pre-defined risk model. There is not a single widely acknowledged privacy risk model, despite the fact that cybersecurity has a widely used risk model based on the risk elements of threats, vulnerabilities, likelihood, and impact. The National Institute of Standards and Technology (NIST) has created a privacy risk model that uses the probability of a problematic data action multiplied by the impact of a problematic data action to determine risk (National Institute of Standards and Technology, 2019). A tool called the Privacy Risk Assessment Methodology (PRAM) has been created by the NIST, which uses the risk model to assist companies in analyzing, ranking, and responding to privacy concerns. The PRAM can promote collaboration and communication amongst a variety of organizational components, including privacy, cybersecurity, business, and IT staff (National Institute of Standards and Technology, 2019).

3.3. Overall Methodology

Organizations should adopt a formal privacy framework for managing privacy risks. Many organizations have introduced frameworks, but they lack guidelines or tools to conduct privacy risk assessments. In this section, we propose a privacy framework as a solution to avoid privacy issues in conference tools. The main phases include analyzing the conference system to detect privacy risks and implementing the proposed framework by applying governance and technical controls to handle privacy issues. The Zoom video conferencing system will be taken as an implementation system to conduct the proposed privacy solution.

The NIST Privacy Framework resembles the NIST Cybersecurity Framework in several respects, including the categorization of privacy functions into five groupings: Identify, Govern, Control, Communicate, and Protect (Figure 8). Like its cybersecurity counterpart, the privacy framework positions risks in easily digestible and common-sense terminology that helps support effective communication with technical and non-technical stakeholders, including executive bodies.

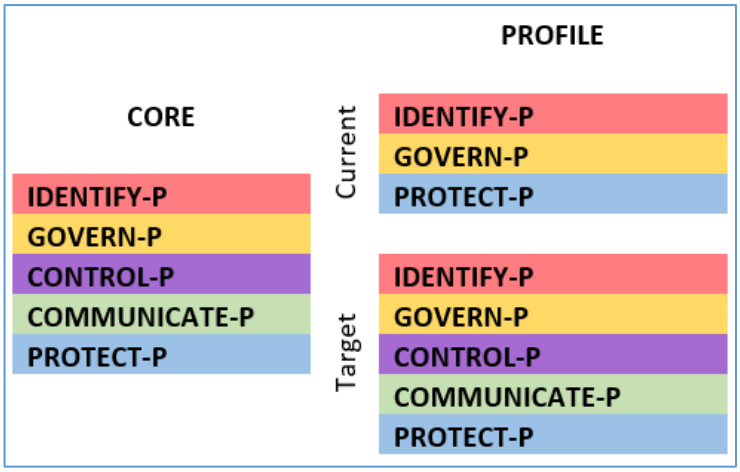

Figure 8: NIST privacy framework core and profile

The NIST Privacy framework helps to capture and quantify privacy risks in such a way that they can be included in the conversation and prioritization models for enterprise risk and given appropriate attention from organizational leadership. Table 2 illustrates the NIST framework with functions and categories showing sample data. Figure 9 illustrates the NIST privacy framework maturity levels.

Table 2: NIST framework with functions and categories showing sample data

Functions	NIST Privacy 1.0 Categories	Target Score	Policy Score	Practice Score
	Overall	**3.00**	**3.17**	**2.83**
IDENTIFY-P	Inventory and Mapping (ID.IM-P)	3.00	5.00	1.00
	Business Environment (ID.BE-P)	3.00	4.00	2.00
	Risk Assessment (ID.RA-P)	3.00	3.00	3.00
	Data Processing Ecosystem Risk Management (ID.DE-P)	3.00	2.00	4.00
GOVERN-P	Governance Policies, Processes, and Procedures (GV.PO-P)	3.00	1.00	5.00
	Risk Management Strategy (GV.RM-P)	3.00	5.00	1.00
	Awareness and Training (GV.AT-P)	3.00	4.00	2.00
	Monitoring and Review (GV.MT-P)	3.00	3.00	3.00
CONTROL-P	Data Processing Policies, Processes, and Procedures (CT.PO-P)	3.00	2.00	4.00
	Data Processing Management (CT.DM-P)	3.00	1.00	5.00
	Disassociated Processing (CT.DP-P)	3.00	5.00	1.00
COMMUNICATE-P	Communication Policies, Processes, and Procedures (CM.PO-P)	3.00	4.00	2.00
	Data Processing Awareness (CM.AW-P)	3.00	3.00	3.00
PROTECT-P	Data Protection Policies, Processes, and Procedures (PR.PO-P)	3.00	2.00	4.00
	Identity Management, Authentication, and Access Control (PR.AC-P)	3.00	1.00	5.00
	Data Security (PR.DS-P)	3.00	5.00	1.00
	Maintenance (PR.MA-P)	3.00	4.00	2.00
	Protective Technology (PR.PT-P)	3.00	3.00	3.00

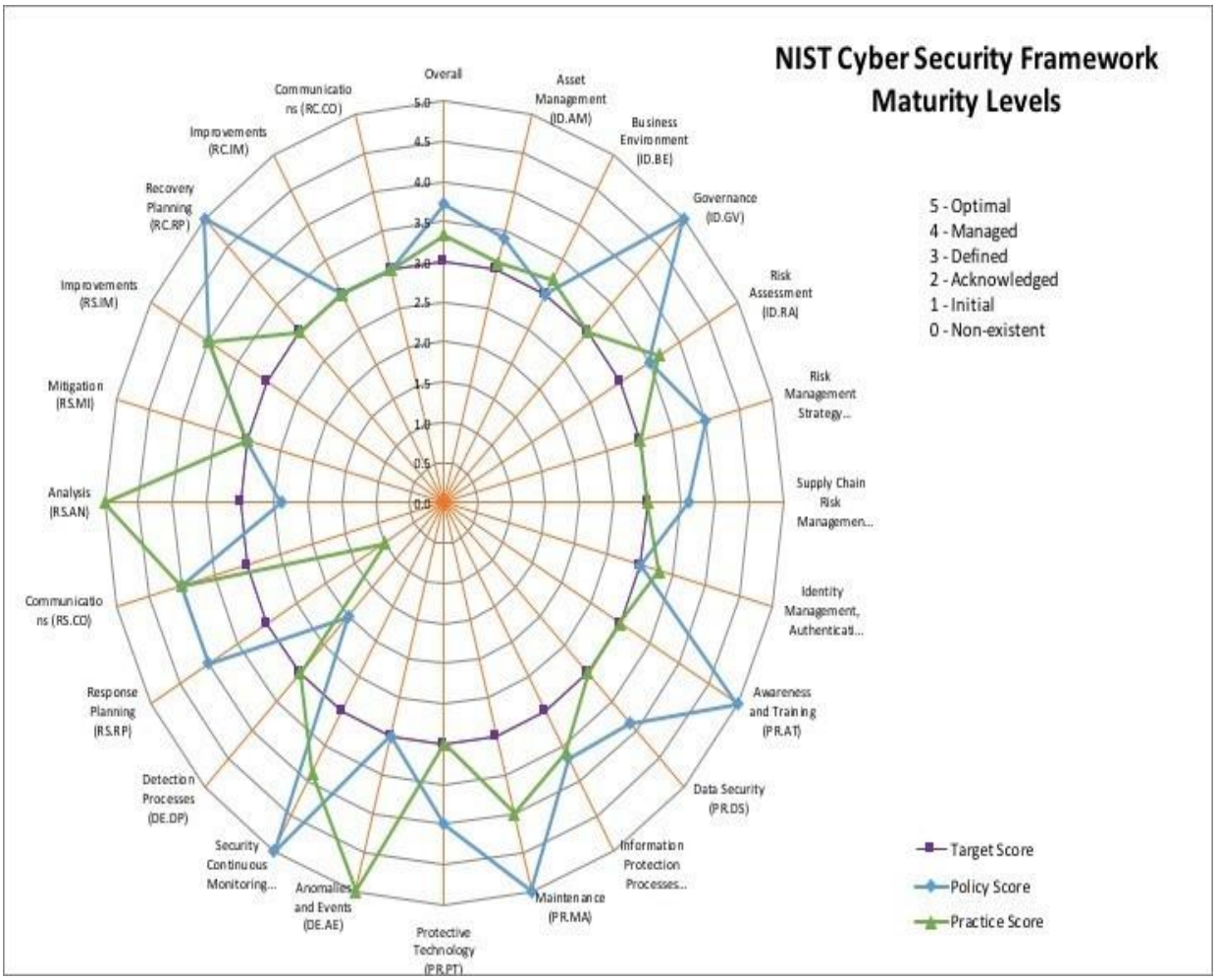

Figure 9: NIST privacy framework maturity levels

Analyze Zoom as a Conference System

In this section, we analyze Zoom to assess the privacy risk. Figure 10 illustrates the current situation in Zoom. The results of the analysis of the Zoom system showed the presence of privacy risks since proper controls are not implemented well. Therefore, we applied the following governance and technical controls to solve the current privacy issues. Figure 11 illustrates the proposed design for Zoom to avoid privacy issues.

Governance

- Define a clear privacy policy.
- Adopt Privacy Risk Assessment Methodology.
- Communicate and document clearly how the PII data is processed.
- Conduct pilot of use cases for continual service improvement (CSI).
- Define cryptography standards based on the nature of the service.

Technical Controls

- Encrypt end-to-end session.
- Enable Auditing.
- Block access to recording meetings without approval.
- Put control on the remote control with consent.
- Manage participants and meetings.
- Use two-factor authentication (2FA).
- Implement role-based access control.

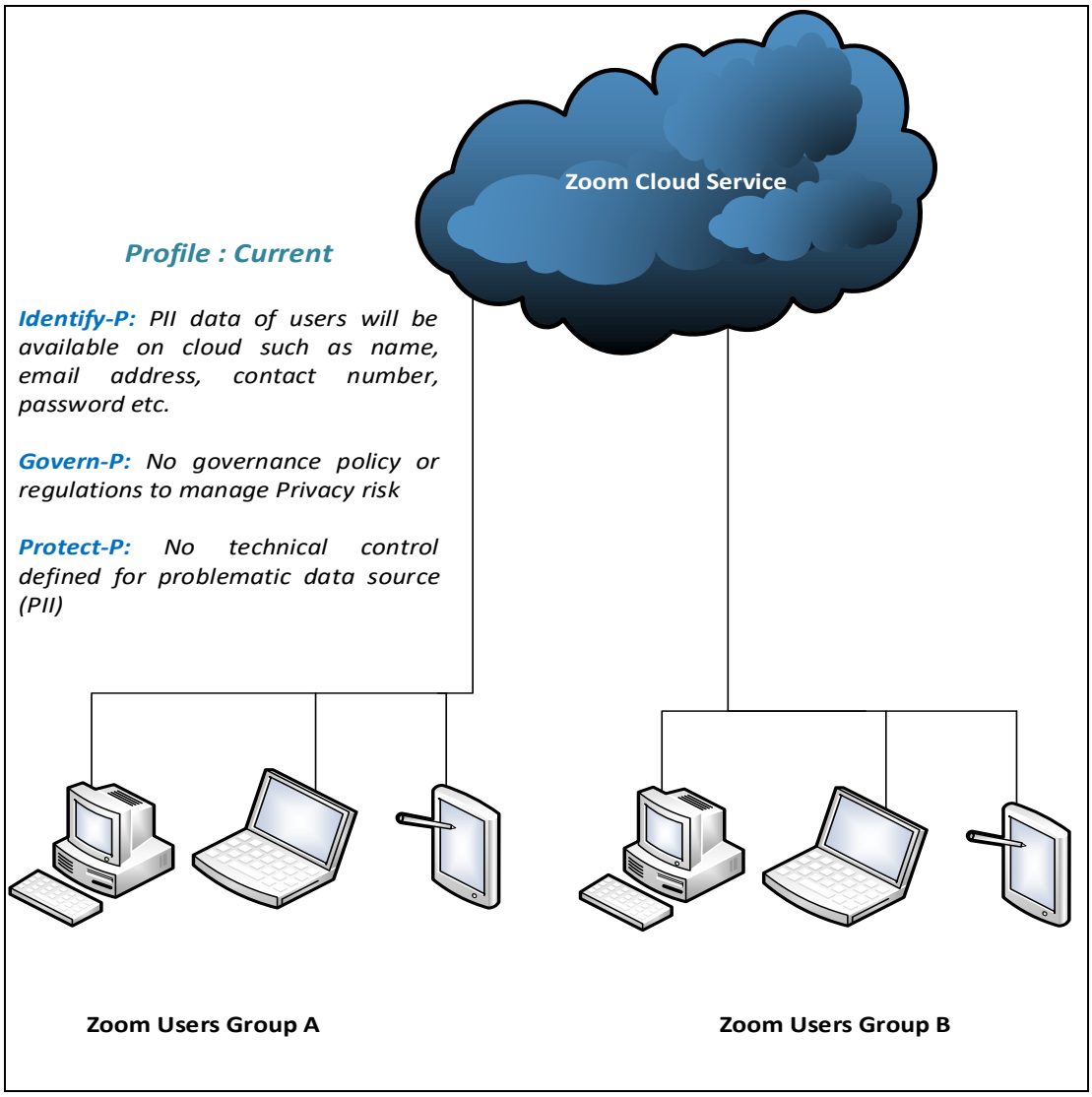

Figure 10: Current Zoom Service

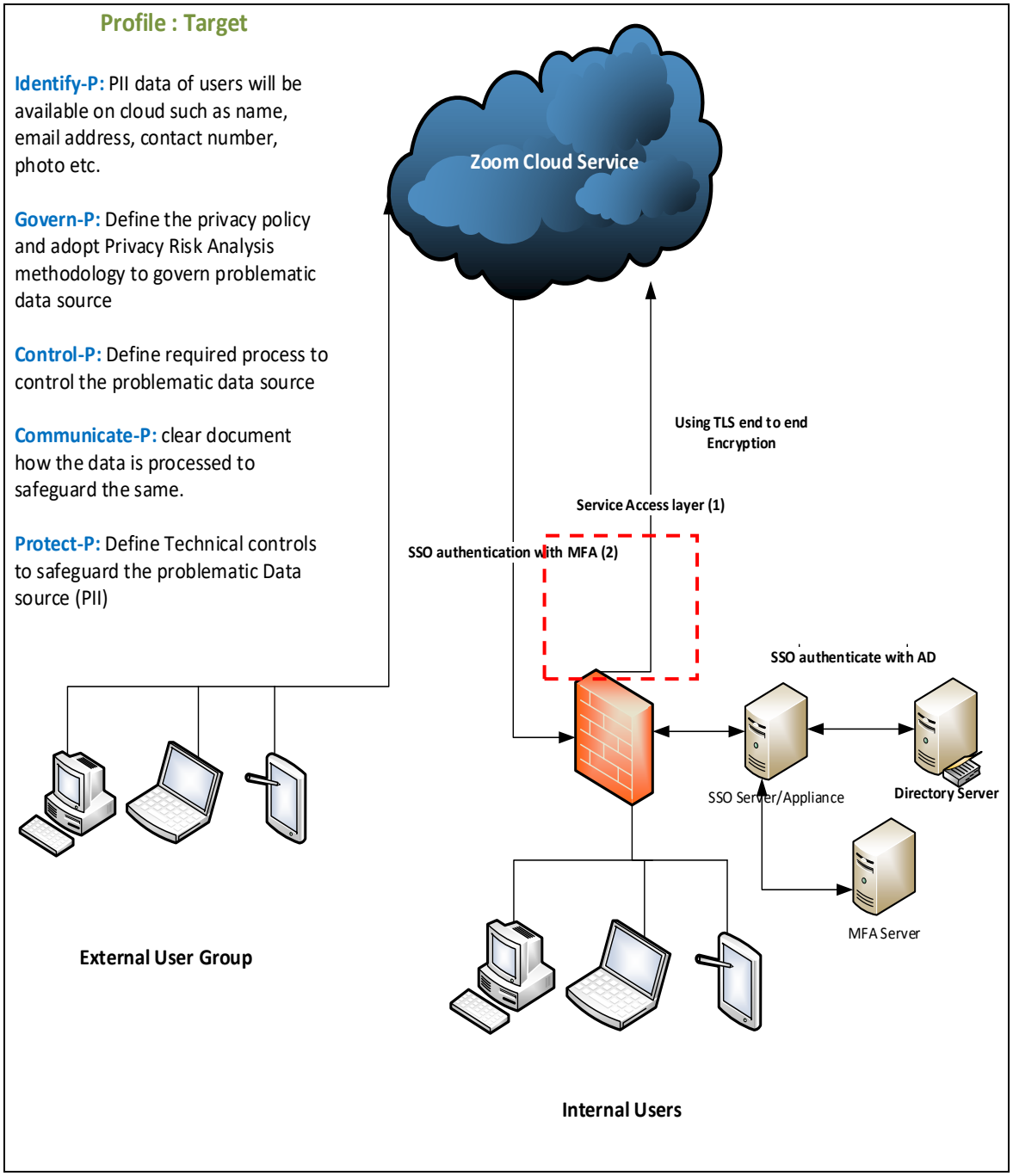

Figure 11: Proposed privacy solution for Zoom

3.4. Implementing the Proposed Framework

This section explores how to implement the suggested privacy solution to handle the privacy issues in the conference systems based on applying the recommended governance and technical controls discussed in the previous section. Figure 12 presents the governance and technical controls adopted in the proposed solution. The following subsections will introduce the adopted controls.

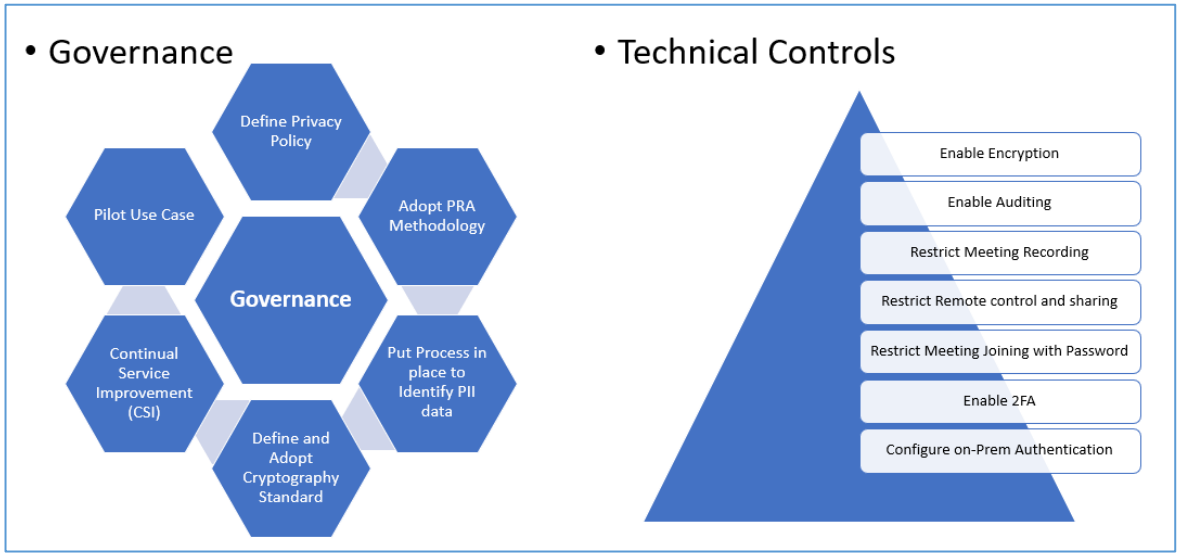

Figure 12: Adopted governance and technical controls

Governance

The implementation of the governance measures that have been implemented to prevent privacy concerns in online conferencing systems will be covered in this part. Cybersecurity governance offers a strategic perspective on how a company manages its security, including defining its risk appetite, constructing accountability frameworks, and identifying decision-makers. Additionally, strong governance will guarantee that cybersecurity initiatives advance the organization's strategic objectives. There are many widely used cybersecurity governance frameworks, such as the one in the NIST framework. Applying the governance policy will be discussed in detail below.

Privacy Policy

The following is the goal of the privacy policy, which was adapted from (ISO/IEC 27001, 2013), which states that it is important for any business to record, keep, process, communicate, and otherwise handle private information about persons. To handle this private information in the right way, a corporation offers fair, secure, and legal solutions. All such company actions are intended to be compliant with acknowledged privacy principles and customary commercial practices. This policy applies to all corporate employees, contractor employees, grantees, sub-grantees, and any other people or organizations involved in managing and safeguarding PII. The Policy Statement is:

- All parties are required to preserve participant PII from unlawful disclosure and to ensure its privacy.
- Every party involved in the grant must make sure that the PII they used was acquired according to all applicable laws and procedures protecting the confidentiality of information.
- Encryption is required for all PII that is sent via email or kept on external storage.
- All PII held on-site must be managed with the proper information technology (IT) services and must always be protected from unauthorized individuals. It is strictly forbidden to access, process, and store personally identifiable information (PII) on privately owned equipment at off-site locations (such as an employee's home and non-grantee-managed IT services, such as Yahoo mail, Gmail, etc.).

- All parties who will have access to sensitive, confidential, proprietary, or private information must be made aware of the information's confidentiality, the precautions they must take to protect it, and the possibility of legal action if the information is improperly disclosed.
- All PII data processing must ensure the confidentiality of the records and documents and be done in a way that makes it impossible for unauthorized individuals to access them through a computer, remote terminal, or any other method.
- Only personnel of the grant recipient who require it in their official capacity to carry out tasks related to the grant agreement's scope of work will be granted access to any PII received via the grant.
- Grantees/subcontractors agree to allow the company to perform onsite audits and/or other investigations during regular business hours to verify that the grantee is adhering to the aforementioned confidentiality obligations. According to this obligation, grantees are required to make this agreement's documents accessible to authorized individuals for inspection, review, and/or audit.
- Grantees/Subcontractors are only expected to keep data they obtain from the company for as long as is necessary to utilize it for assessments and other reasons, or as long as is necessary to meet any applicable corporate records retention obligations. Following that, the grantee concurs that all data will be destroyed, including any electronic data that has been deleted.
- Before obtaining PII or sensitive information from participants, request that they sign releases confirming that PII would only be used for grant-related activities. The grantee agrees to delete all electronic data after which all data will be destroyed. PII must be kept or displayed in a form that cannot be used to identify a specific person.
- Use the right techniques to securely delete sensitive electronic PII and shred sensitive paper PII from files.
- Do not leave records containing PII open and unattended.
- Use suitable procedures for erasing sensitive PII in paper files, such as shredding and securely deleting sensitive electronic PII.
- Immediately disclose any PII violation, whether actual or suspected.
- Individuals' personal information must not be stored in a way that makes it possible to identify them for any longer than is required for the purposes for which it was acquired or for which it is further processed.
- Personal data must be protected with adequate and authorized cryptographic controls both in transit and at rest, such as the Advanced Encryption Standard (AES256) encryption method and the Transport Layer Security (TLS) 1.2 protocol.
- To prevent brute force attacks, use two-factor authentication (2FA) on the signature page.
- The business retains the right to keep tabs on the actions of any employees, contractors, or other parties involved in processing personally identifiable information, including but not limited to email, internet access, or archived data.
- Personal data may only be processed if:
    - The person has expressly given consent.
    - Processing is necessary to fulfill the person's request.
    - Processing is required to fulfill a contractual obligation owed by the Owner.
    - Processing is necessary to research or provide new business products or services that would be beneficial to the owner, provided that these new products or services do not exceed the individual's fundamental rights or freedoms.
    - Processing is necessary to safeguard the person's vital interests.

Disciplinary actions, including termination of employment, may follow any breach of this policy. The organization reserves the right to report any illegal activity to the relevant law enforcement agencies and to assist with any subsequent investigations. The organization does not regard behavior that violates

this policy to be part of an employee's or partner's course and scope of employment or to be a natural outgrowth of the performance of their obligations. The organization maintains the right, to the fullest extent permissible by law, not to defend or pay any damages imposed against employees or partners as a result of a violation of this policy.

Cryptography Policy

On computer networks, confidential discussions and transactions must be protected throughout electronic communications. This issue has a solution, which is cryptography. The cryptography policy's goal is to make sure that any organization is effectively using cryptography to safeguard the privacy, veracity, and/or integrity of data. This policy applies to the company's data processing and process control systems that have or use information and/or facilities owned by the company. In addition. This policy applies to all employees, partners, and third parties with access to the company information assets regardless of geographic location. The control techniques adopted for each data area (in use, in transit, at rest) are shown in Table 3 (Gary, 2022).

Table 3: Data area (Gary, 2022)

Area	Control Techniques
Data in Transit	Using TLS 1.2 protocol
Data in Use	This is applied on DB level encryption when in use.
Data at Rest	Encryption on disk or server. In our case, we will use end-to-end encryption to achieve

The policy statement for data in use as adopted from (ISO/IEC 27001, 2013) is:

1. Encryption controls shall be implemented as required on critical business applications accessible over the Internet or any systems that might have sensitive information.
2. Import, export, and use of encryption methodologies shall comply with applicable laws and regulations.
3. Users shall exercise caution when signing and encrypting messages depending on the sensitivity of messages.
4. Users are not permitted to employ encryption, digital signatures, or digital certificates for any business activity or business information without the written authorization of their department manager. Before they utilize these complex technologies, users must also be properly trained, and their systems must be configured by authorized personnel.
5. If secret information is to be stored on a multi-user computer system, it must be compressed and then encrypted using an approved encryption algorithm.

In addition, for the data at rest, the following cryptography policy is applied:

1. Any confidential and restricted Information pertaining to business stored in the designated folders shall be encrypted using an approved encryption algorithm.
2. Any sensitive/confidential data at rest should be encrypted.
3. Removable media, including but not limited to CD-ROMs, DVDs, backup tapes, and USB memory drives that contain confidential and restricted information, shall be encrypted using an approved encryption algorithm.
4. The Database encryption strategy shall be formulated based on the criticality of the system and the performance requirement.
5. The key to encrypt data shall be stored separately from the encrypted database. Wherever possible, usage of a hardware storage module shall be considered for storing encryption keys.
6. The access to the key used to encrypt the database shall be highly restricted.

For the data in transit, the following cryptography policy is applied:

1. Data transferred through the Internet shall be adequately protected with suitable encryption technologies according to the key management requirements.
2. Any confidential and restricted information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business shall be encrypted or transmitted through an encrypted tunnel.
3. Transmitting unencrypted confidential and restricted information through web email programs shall not be allowed.

Techniques for Selection Policy

The choice of which particular techniques will be used must be made after the risk assessment has determined the overall necessity for using cryptography (ISO/IEC 27001, 2013). Using the technique will also require the choice and the purchase of software or hardware. Here, the choice of such methods must take into account any national or current legal limitations on the acquisition and use of cryptographic technology. The technique selection policy for the applicable business process or circumstance is shown in Table 4.

Table 4: Selecting Policy Technique (ISO/IEC 27001, 2013)

Process/Situation	Technique	Type
Website Security	TLS 1.2 “Transport layer security”	Protocol
Protection of data on removable media	AES 256 “Advanced encryption standard “	Encryption Algorithm
Email Security	S/MIME “Secure / Multipurpose Internet Mail Extension”	Encryption Algorithm
Remote Access	Virtual Private Network (VPN) using TLS 1.2	Protocol

Technical Guidelines for the Privacy Policy

In addition to the privacy and cryptography policies discussed above, there is basic guidance on how to protect user privacy and the privacy of others when using any remote meeting tool (Zoom, 2021). The guidance includes technical tips for the visibility of remote locations, screen sharing privacy, managing participants and meetings, and recording meetings and chats.

Technical Controls

This section will explore implementing the adopted technical controls to avoid privacy issues in online conference systems. As mentioned above, the Zoom conference system was used as an implementation environment. The adopted technical controls are:

- Encrypt end-to-end session.
- Enable Auditing.
- Block access to recording meetings without approval.
- Put control on the remote control with consent.
- Manage participants and meetings.
- Use two two-factor authentication (2FA).
- Implement role-based access control.

Encryption

To ensure confidentiality, which is one of the important pillars in computer network communications, in which unauthorized access is prevented, individuals must have a method to guarantee the security of their conversations and transactions. Cryptography offers a solution for this matter. Encryption essentially involves only the intended recipient, possessing the correct decryption key, who can access the content. This provides a means to protect your conversations from access by hackers, intruders, advertisers, or other entities. Encryption guarantees confidentiality for data, whether the status of data is at rest or during transit.

Moreover, the implementation of chat encryption ensures the transmission of chat messages among Zoom users. This encryption technique utilizes TLS 1.2 and the AES 256-bit algorithm to encrypt all chat messages. AES, known as the Advanced Encryption Standard, is widely recognized as a secure encryption algorithm. It operates symmetrically, meaning both the sender and receiver employ the key for both encryption and decryption processes with a length of 256 bits. By enabling chat encryption, data, at rest and during transit, receives protection.

Auditing and Monitoring

Auditing, known as operation logs in Zoom's terminology, plays a role in ensuring that the platform maintains accountability. It allows administrators and all users to accurately track and review their actions. Administrator operations are thoroughly documented, including details like the time stamp, the responsible administrator, the action category, and specific information related to the action taken. Additionally, privacy controls require monitoring of security logs. Zoom simplifies this process by providing a RestAPI for integration with Security Information and Event Management (SIEM) solutions, as shown in Figure 13 (Zoom Developer Docs. 2022). This robust auditing framework not only enhances the trustworthiness of user actions but also establishes accountability within the system.

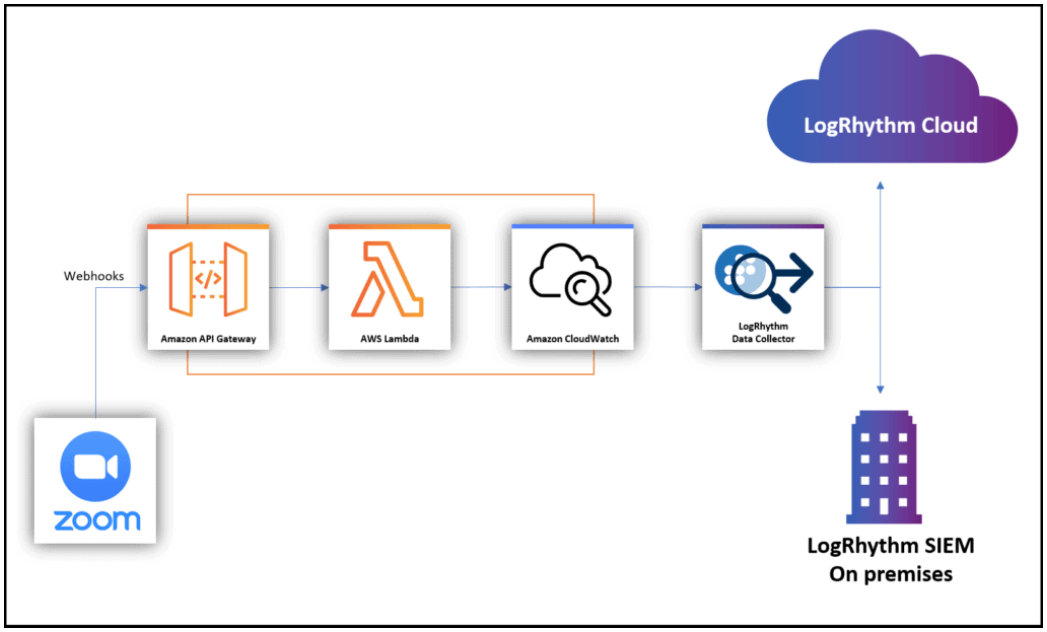

Figure 13: Monitoring zoom activity using zoom rest API webhook in LogRhythm SIEM (Zoom, 2021)

Block Access to Recording Meetings Without Approval

This involves implementing measures to prevent individuals from recording meetings unless explicit approval has been granted. Requiring approval ensures that participants are aware of and consent to the recording. This aligns with privacy regulations and compliance standards, promoting ethical and legal practices. Therefore, a secure approach involves giving the host the authority to enable recording when it is genuinely necessary. Failing to restrict recordings can lead to privacy issues and the misuse of sensitive information. By requiring approval before recording, organizations can proactively safeguard the integrity of their meetings and maintain the confidentiality of shared information.

Put Control on the Remote Control with Consent

Before allowing remote control in Zoom session, the user must approve the action to have remote control. In addition, disabling screen sharing, by default, will protect from the accidental sharing of sensitive data.

Managing Participants and Meetings

Adding a password to our meetings is a step in ensuring the security of our sessions. When participants are required to enter a password before joining, it adds a layer of defense against entry. Additionally, we enhance security by having the host approve anyone who wants to join the meeting. The combination of password protection and host approval creates an environment for collaboration, assuring participants that their interactions will remain private and confidential.

Two-Factor Authentication (2FA)

Utilizing 2FA guarantees authenticity. Two-factor authentication ensures that the person accessing data is known and verified using a two-factor token or SMS. It adds a layer of verification to make it more challenging for individuals to gain access. It makes it harder for attackers to gain unauthorized access. Enabling the 2FA can be done via a phone number that can receive an OTP as an SMS, an authentication app such as Microsoft Authenticator or Google Authenticator, or a working email address.

Role-based Access Control

After authenticating and verifying the user's identity, a user is then granted access to the data. Role-based access control is one of the models where access rights are granted based on users' roles. For instance, the host will have more privileges than a guest. Utilizing role-based access, two important security design principles are compiled: least privilege and segregation of duties. In the least privilege, the least access rights are granted to allow an individual to do the task, whereas, in segregation of duties, more than one person is needed to complete a task. Therefore, if no one person has complete access control or full authorization, this would reduce the misuse, sabotage, and theft of information.

4 Research Results and Discussions

This research aimed to propose a privacy framework to handle privacy issues in conference systems by applying governance and technical controls. This section presents the research results after applying the adopted privacy controls. Section 4.1 presents the results of implementing the governance policies, while Section 4.2 presents the results of implementing the technical controls.

4.1. Results of Implementing Governance Policies

By implementing the governance privacy controls, several benefits were achieved.

1. Increased Trust and Credibility

The organization applied the governance privacy controls to gain customer trust and credibility since it follows the privacy principles in making decisions regarding data protection.

2. A Better Understanding of the Collected Data

The adoption of privacy standards gives businesses a greater understanding and appreciation of their data and how it moves throughout the organization. When employees know that an organization has a demonstrable commitment to privacy and the security of their personal data, from how long it is retained to how it is disposed of, they feel more confident and secure about their workplace.

3. Improved Data Management

Examine the data you gather, how much of it is collected, and the purposes for which it is used. This will give you a foundation for what data you can keep collecting and what to stop gathering, which will improve your data management.

4. Enterprise Brand Reputation

Without a proven commitment to privacy, firms risk brand damage and criticism that their goods and/or services are sneaky or creepy. Privacy is essential to building trust. Organizations can avoid potential fines and uncover hidden brand and reputational value by maintaining privacy.

5. Competitive Benefits

The organization adopted privacy principles, and getting certified gives an advantage over other organizations when it comes to competition. Customers will have more trust in organizations that comply with privacy standards.

4.2. Results of Implementing Technical Controls

Table 5 compares the before and after implementation of the proposed framework based on technical controls.

5 Conclusions, Recommendations, and Future Work

This section concludes the paper and presents recommendations and possibilities for future work.

5.1. Conclusions

Despite having several privacy protections in place, Zoom still needs to implement governance guidelines and technical controls to enforce them. Every business and individual working with personally identifiable information can benefit greatly from implementing and maintaining a privacy framework based on the industry standard, such as the ISO/IEC 27001 standard or the NIST privacy framework. Additionally, the privacy framework will help to enhance privacy, support good governance,

save overhead expenses associated with security, and act as a smart marketing approach to boost your credibility with widely accepted standards. Zoom's conferencing system has privacy issues that must be addressed to protect the users' data. This paper proposed a framework to address Zoom's privacy issues by applying a set of governance and technical controls. The proposed solution significantly addresses Zoom's privacy issues.

Table 5: A comparison of before and after implementing the technical controls

Area of controls	Before	After
Encryption	Without enabling encryption, Zoom data will transfer over the network in plain text, any man-in-the-middle attack can gain access to data and can misuse and cause damage to the organization's reputation and result in huge penalties.	Adopting strong encryption standards leads to protecting the data at rest and in transit. Even man in the man-in-the-middle attacker gained access to Zoom data, which is no use because it is encrypted.
Auditing	Without enabling proper auditing, it is difficult to monitor the activity of Zoom data accessed.	Monitor the detailed activity of Zoom data accessed and get visibility.
Recording of Meeting/Chat	Not restricting Zoom meetings or chats can lead to privacy issues, and people might misuse information.	After implementing controls by default, Zoom meeting/Chat recording is disabled. Based on need, the host can enable the recording.
Screen Sharing Privacy	By default, screen sharing is allowed in most video conferencing solutions.	Disabling screen sharing in video conferencing by default will protect the accidental sharing of sensitive data. It should be allowed based on a need-to-have basis.
Managing Participants and Meetings (Restrict Meeting Joining with Password)	Before implementing the proposed controls, anyone who knows the meeting ID can join without the host's approval. This can lead the attacker to steal the Zoom data.	With adopted the proposed controls, each meeting is protected. Also, the host must approve if anyone asks to join the meeting. This approach helps the organization protect its users' privacy and confidentiality.
2FA	Not enabling the 2FA for the sensitive login data can lead to an easy brute-force attack.	Enabling the 2FA in the Zoom system makes it difficult for the attacker to access sensitive data.
Role-Based Access Control (Configure on-prem authentication)	Not implementing the role-based access control will deviate from the principle of segregation of duties and least privilege. Too many people having admin access can lead to more security breaches.	Implementing role-based access control and granting controlled access will reduce security breaches.

5.2. Recommendations

Organizations conducting online meetings should adopt a formal privacy framework for managing privacy risks. Many organizations lack guidelines/tools to conduct privacy risk assessments. As recommendations, we suggest the following points:

1. Develop enterprise personal information asset and risk inventory.
2. Release a privacy policy.
3. Build use cases for privacy measurement and do pilot testing from time to time to improve further.
4. Form a cross-agency data privacy steering group/committee to provide insight on developing privacy principles, policy, impact assessment, and training.
5. Privacy risk assessment should be divided into the information gathering and risk assessment phases.

5.3. Future Work

While the proposed framework offers a promising solution to address the privacy issues in the conference systems, information privacy research should focus on finding the gaps and misuse of data collected. We recommend that future research consider different levels of analysis and the multilevel effects of information privacy in different areas, not only in specific areas. Future businesses will heavily rely on consumer/public data, where public data is key in doing business and needs to be taken very seriously to protect it.

References

[1] Aiken, A. (2020). Zooming in on privacy concerns: Video app Zoom is surging in popularity. In our rush to stay connected, we need to make security checks and not reveal more than we think. *Index on Censorship, 49*(2), 24-27.

[2] Botacin, M., Judd, M., Lange, A., Li, T.C., & Salathé, M. (2021). Does Your Threat Model Consider Country and Culture? *A Case Study of Brazilian Internet Banking Security to Show That It Should!*.

[3] Botha, R., & Furnell, S. (2021). Facing up to security and privacy in online meetings. *Network Security*, *2021*(5), 7-13.

[4] Cobo, C., & Vargas, P.R. (2022). Turn off your camera and turn on your privacy. *Learning to Live with Datafication: Educational Case Studies and Initiatives from Across the World*..

[5] Dean, B. (2021). Zoom user stats: How many people use zoom in 2022. https://backlinko.com/zoom-users

[6] Djeki, E., Degila, J., Bondiombouy, C., & Alhassan, M.H. (2021). Security Issues in Digital Learning Spaces. *In IEEE International Conference on Computing (ICOCO)*, 71-77.

[7] Goodyear, M. (2019). The dark side of videoconferencing: The privacy tribulations of Zoom and the fragmented state of US data privacy law. *HLRe: Off Rec.*, *10*, 76.

[8] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) (2013) ISO/IEC 27001 : 2011 – Information technology – Security techniques – Privacy framework (ISO, Geneva, Switzerland). https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_27001_2011.zip

[9] Isobe, T., & Ito, R. (2021). Security analysis of end-to-end encryption for zoom meetings. *IEEE access*, *9*, 90677-90689.

[10] Kagan, D., Alpert, G.F., & Fire, M. (2020). Zooming Into Video Conferencing Privacy. *IEEE Transactions on Computational Social Systems, 11*, 933-944.

[11] Kessler, G.C. (2003). An overview of cryptography. https://www.garykessler.net/library/crypto.html

[12] Mahr, A., Cichon, M., Mateo, S., Grajeda, C., & Baggili, I.M. (2021). Zooming into the pandemic! A forensic analysis of the Zoom Application. *Forensic Science International: Digital Investigation, 36*, 301107 - 301107.

[13] Mohanty, M., & Yaqub, W. (2020). Seamless authentication for online teaching and meeting. *IEEE Sixth International Conference on Multimedia Big Data (BigMM)*, 120-124.

[14] National Data Management Office. (2022). https://sdaia.gov.sa/en/Sectors/Ndmo/Pages/default.aspx

[15] National Institute of Standards and Technology. (2019) NIST Privacy Risk Assessment Methodology (PRAM). https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[16] Park, M., Kim, S., & Kim, J. (2020). Research on Note-Taking Apps with Security Features. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 11*(4), 63-76.

[17] Singh, J., & Chaudhary, N.K. (2022). OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities. *Journal of Information Security and Applications, 65*, 103091. https://doi.org/10.1016/j.jisa.2021.103091
[18] Singh, R., & Awasthi, S. (2020). Updated comparative analysis on video conferencing platforms-zoom, Google meet, Microsoft Teams, WebEx Teams and Go To Meetings. *Easy Chair Preprint, 4026*, 1-9.
[19] Susukailo, V., Opirskyy, I., & Vasylyshyn, S. (2020). Analysis of the attack vectors used by threat actors during the pandemic. *IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), 2*, 261-264.
[20] Weise, E. (2022). 43% of companies had a data breach in the past year. https://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/
[21] Zoom Developer Docs. (2022). https://developers.zoom.us/docs/api/
[22] Zoom Video Communications. (2021), How virtual do we want our future to be?. https://explore.zoom.us/docs/en-us/future-of-video-conferencing.html

Authors Biography

Samer Atawneh received his PhD Degree in information security from Universiti Sains Malaysia (USM) in 2015. Currently, Dr. Atawneh is an Associate Professor at the College of Computing and Informatics, Saudi Electronic University, Saudi Arabia. He has published several research papers in international journals and conferences with high reputation, where most of these publications are tracked by Thomson Reuters (ISI) and Scopus. His research interests lie in information security, steganography, software engineering, machine learning, mobile applications, and optimization.

Ziad Alshammari received his master's degree in cybersecurity from Saudi Electronic University in 2022. Currently, Alshammari is working as a strategic general manager with over 12 years of experience. He can analyze market trends, identify growth opportunities, and develop and execute strategic plans to achieve business objectives**.** In addition, he has a strong background in product development and innovation and experience building innovative products that support the overall business strategy. He has a deep understanding of customer needs and preferences and uses this knowledge to develop products and services that meet those needs and differentiate the organization from its competitors.

Mousa AL-Akhras obtained his B.Sc. and M.Sc. degrees in computer science from the University of Jordan, Amman, Jordan, in 2000 and 2003, respectively. He earned his Ph.D. degree in 2007 from De Montfort University, Leicester, UK. His Ph.D. specialization is artificial neural networks & communications. He was promoted to associate professor in 2012. From 2014 to 2022, he joined Saudi Electronic University (SEU) as the coordinator for M.Sc. In Cyber Security Program. In October 2022, he returned to the University of Jordan. His research interests include problems in artificial neural networks and their applications in security, business, and health.

Bayan Abu Shawar holds a BSc and a Master's degree in Computer Science from the University of Jordan and a Ph.D. from the School of Computing at the University of Leeds. Currently, she is an Associate Professor in the Cybersecurity Department in the Faculty of Engineering at AL Ain University. Before Joining AL Ain University, she was an Associate Professor at Arab Open University in Jordan. Her research interests include Chatbots, Natural Language Intelligence, Information Retrieval, Artificial intelligence, e-learning, Question Answering systems, and Learning Management Systems.