End-to-End Encryption: Technological and Human Factor Perspectives

Leandros Maglaras and Kitty Kioskli(✉)

trustilio, B.V., Amsterdam, The Netherlands
{leandros.maglaras,kiity.kioskli}@trustilio.com

Abstract. End-to-end encryption (E2E) has become a cornerstone of modern digital communications, safeguarding data from unauthorized access during transmission. E2E encryption ensures that only the intended recipient can decrypt the data, keeping it invisible even to service providers. However, this technology presents a paradox: while it protects individual privacy and fosters trust in digital systems, it also challenges law enforcement agencies by creating potential safe havens for illegal activities. This paper explores the dual nature of E2E encryption, its significance for privacy, and the various threats it poses, and presents some recent innovative solutions aimed at addressing these challenges.

Keywords: E2EE · Human Factors · Privacy

1 Introduction

Encryption is crucial for maintaining security and privacy in the digital world. It ensures that sensitive information, such as personal data, financial transactions, and private communications, is protected from unauthorized access. By converting data into unreadable code, encryption makes it accessible only to those with the correct decryption keys, safeguarding it from hackers, identity thieves, and other malicious actors. This layer of protection is essential for individuals, businesses, and governments to prevent data breaches and keep confidentiality. In an age where cyber threats are increasingly sophisticated, encryption not only reassures privacy preservation but also enhances trust in digital services and communication platforms. Trust is the most important aspect of digital services since the loss of it from the users will lead to collapse of modern societies [1].

End-to-end encryption (E2EE) stands as one of the most important advancements in securing digital communications. This technology ensures that messages, files, and other forms of data can only be accessed by the intended sender and receiver, leaving no room for third parties—even the service providers themselves—to intercept or decipher the content. In an era where data breaches and digital surveillance are prevalent, E2EE serves as a vital solution for securing both individual and organizational privacy [2].

The increasing reliance on digital communication for personal, professional, and governmental purposes has highlighted the importance of the application of robust

D. D. Schmorrow and C. M. Fidopiastis (Eds.): HCII 2025, LNAI 15778, pp. 129–139, 2025.
https://doi.org/10.1007/978-3-031-93724-8_10

encryption methods. From instant messaging applications to cloud storage platforms, E2E encryption has become a provider of trust for the end users. Recently, FBI and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a warning to smartphone users about the risks associated with sending unencrypted text messages between iPhones and Android devices. These unencrypted messages are vulnerable to interception by cybercriminals, potentially exposing sensitive information [3] (Fig. 1).

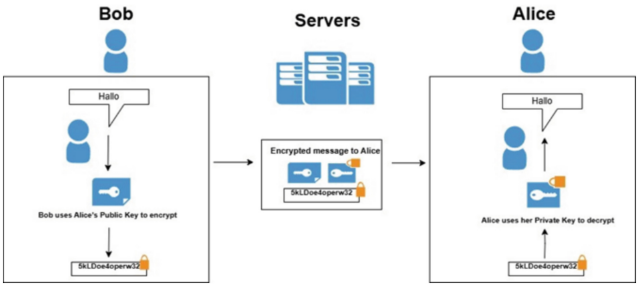

Fig. 1. End to End reception. Mechanism.

However, this same technology has initiated a huge debate over its implications for law enforcement and national security [4]. Critics argue that encryption can provide a safe environment for criminal activities, complicating investigations and undermining public safety [5]. Access to data is important to law enforcement agencies for both proactive and reactive actions against cybercriminals. Reactive actions mainly refer to the capacity of technology companies to respond to law enforcement investigations by providing data from suspected criminals on their platforms. Proactive actions stand for the ability of technology companies to actively identify illegal and harmful activities on their platforms, particularly in detecting users with a sexual interest in children. As stated in the Joint Declaration of the European Police Chiefs [5], they are concerned that the implementation of end-to-end encryption is being carried out in a manner that will undermine both of these capabilities.

Privacy, a fundamental human right, is tightly linked to encryption. In an interconnected world, sensitive data—including personal habits, health information, and social interactions—is constantly at risk of exposure. E2EE helps safeguard this information from unauthorized access [6]. Nevertheless, its implementation raises ethical questions about the balance between individual privacy and collective security, particularly when encryption blocks the detection of illegal activities [7].

While E2EE is designed to be user-friendly, many individuals may not fully understand how encryption works or the importance of keeping their encryption keys secure. This lack of knowledge can lead to incorrect usage or weak implementation of the offered solutions. Users can be vulnerable to phishing attacks, social engineering, or other forms of manipulation that bypass encryption [8]. Mobile communication devices are vulnerable to physical over-the-shoulder eavesdropping as well as digital eavesdrop-ping often via unknown malware infections [9]. Effective education and awareness are crucial for ensuring that encryption's technological benefits are not lost due to human-related vulnerabilities.

Moreover, social media and communication apps are the most frequently consumed application types. However, downloaded apps may hide stalkerware; a category of spyware that enables threat actors to monitor activity and access personal information [10]. Notably, they may be used to allow for Intimate Partner Stalking (IPS) where perpetrators use stalkerware as a surveillance tool against current or previous partners, perpetuating violence against women and girls. Contemporary E2EE is failing to protect privacy, enabling mal actors to spy on their targets.

As stated, E2EE has its limitations. Traditional implementations often fail to address endpoint vulnerabilities, exposing users to malware, spyware, and other threats. Using several existing messenger applications like Signal where data are not backed up or stored reduces the chance of messages being accessed, but the main problem of the data being created and consumed in cleartext on end devices remains. These shortcomings highlight the need for comprehensive solutions that extend protection to the end devices (e.g., mobile phones) where data is created and consumed. This gap in traditional encryption models is an important point of ongoing research and development efforts [11].

In this article, we investigate the current landscape of E2EE solutions, examining their role in securing digital communications and protecting user privacy while addressing current ethical challenges. We briefly present privacy considerations that include location, state of body & mind, social life, behavior & action, and media. Also, we present all emerging threats that are mostly related to insecure third-party apps, human factor, and client-side scanning (CSS) solutions. Moreover, we present state-of-the-art novel solutions related to E2EE that combine augmented reality technology [12] or encrypted keyboard technologies [13]. Finally, we discuss ethical problems and law enforcement dilemmas when dealing with public and most importantly children's safety. By exploring the vulnerabilities inherent in existing systems and human factors related to cybersecurity attacks, this work highlights the need for innovative frameworks. The paper aims to contribute to the ongoing dialogue on how to balance privacy, security, human factors, ethical dilemmas and technological advancements in the modern digital world.

2 Privacy Considerations

Privacy is multifaceted, encompassing aspects such as location, social interactions, behavior, and personal media. Each of these dimensions is vulnerable to surveillance and misuse in the absence of robust protection mechanisms.

2.1 Privacy of Location

Spatiotemporal data, which captures both the location and the timing of an individual's movements, can provide insights into their personal life. By tracking where and when a person goes, this data can reveal sensitive information such as home and work addresses, travel patterns, or visits to specific locations like medical clinics or confidential meetings. While this data can be useful for services like navigation or location-based recommendations, it also presents significant privacy risks, as it can inadvertently expose personal details that individuals may wish to keep private.

When spatiotemporal data is correlated with other datasets, the potential for revealing even more intimate information increases. For example, combining location data with health-related information could expose a person's medical conditions, such as frequent visits to a particular hospital or clinic. Furthermore, cross-referencing such data with social media activity or other digital traces could uncover a person's social circles, daily habits, or even political affiliations. As a result, spatio-temporal data represents not only a powerful tool for businesses and services but also a potential vulnerability to privacy breaches, making it crucial to handle and protect such information with the utmost care. For that reason, several novel privacy preservation mechanisms that can preserve service levels while protecting sensitive users' data [14, 15].

2.2 Privacy of State of Body and Mind

In order to increase the security, many applications use biometric data of the users. Unfotrunately, biometric data, mental states, and political opinions are becoming increasingly vulnerable to breaches, posing serious risks to individual privacy and security [16]. Biometric data, such as fingerprints, facial recognition, or voiceprints, is uniquely tied to an individual and is often used for authentication purposes. However, if this data is compromised, it can be exploited for performing several attacks. Similarly, personal information about one's mental health or political opinions, which can be inferred through digital behavior, is also at risk. A breach of such sensitive data can have far-reaching consequences, from personal discrimination to more systemic exploitation.

The exploitation of this sensitive information could have devastating impacts. Authoritarian governments might use these data to monitor, control, or suppress individuals based on their political views or mental health status, leading to social and political persecution. Personal data may be used to target vulnerable individuals with manipulative marketing tactics or even make discriminatory decisions in hiring or lending practices. The growing exposure of these data types underscores the urgent need for stronger privacy preservation protocols and policies, and ethical guidelines to safeguard against misuse and ensure that personal freedoms are respected [17].

2.3 Privacy of Behavior and Actions

Hobbies, shopping habits, and social media activities collectively create a detailed profile of an individual's life. This data can be collected through various methods, including cookies [18], pixels [19], and specific software development kits (SDKs). These data entries reveal personal preferences, routines, and behaviors, offering insights into who a person is and what they value. Companies and platforms use this information to tailor experiences, target advertisements, and predict future choices. While such personalization can enhance convenience, it also comes with significant security risks and privacy violation tactics.

Violation of users' data privacy can lead to manipulation, social profiling, and repetitive targeted advertising. When personal information is misused or exposed, individuals may be subject to manipulation or even discrimination based on their profiles. This level of intrusion raises concerns about autonomy and ethical data use, highlighting the importance of safeguarding personal information in an increasingly digital world [20].

2.4 Media Privacy

Unauthorized redistribution of photos, videos, or audio files constitutes a direct violation of privacy and intellectual property rights. When such content is shared without consent, it can lead to serious personal harm, including emotional distress, reputation damage, and breaches of confidentiality. This misuse can affect individuals' relationships, careers, and personal security, as sensitive information becomes accessible to unintended audiences.

Beyond personal impact, these violations often carry significant legal consequences [21]. Many jurisdictions have strict laws against unauthorized sharing of media, resulting in potential fines, lawsuits, or even criminal charges.

3 Threats and Challenges

Despite its advantages, E2E encryption has limitations, particularly when it neglects human factors or device vulnerabilities. Mobile devices, which are integral components for communication, often become gateways for attackers through malware, spyware, or stalkerware. These threats are combined with those coming from insecure third-party apps [22].

3.1 Malware and Stalkerware

Malware, including banking trojans and ransomware, are significant threats to mobile device security since they can exploit vulnerabilities and bypass encryption at endpoints. These malicious programs are designed to gain unauthorized access to sensitive information, steal financial data, and even disrupt normal system operations when needed. Banking trojans are particularly dangerous because they target financial institutions and may disrupt online transactions.

Ransomware, which is ranked as the most dangerous threat from the ENISA threat landscape of 2024 [23], locks users out of their data, demanding payment for its release. The ability of these malware types to bypass encryption protocols further complicates efforts to protect users, as attackers can exploit gaps in security and target individuals or organizations with devastating consequences [24].

Stalkerware, a type of surveillance software used to monitor individuals without their consent, is becoming an increasingly alarming issue with serious societal implications. This software is often used to track the activities, whereabouts, and personal communications of partners, raising serious concerns about privacy of individuals' data. In the UK, nearly 5% of adults admit to using such apps, which underscores the growing prevalence of this invasive behavior. The impact of stalkerware extends beyond individual privacy violations, as it can lead to emotional abuse, manipulation, and control within relationships. The societal implications of stalkerware highlight the need for stricter regulations and awareness surrounding digital privacy and personal security.

3.2 Human Factor

While data may be encrypted during transmission, endpoints often lack adequate protection. Cleartext consumption of data on devices makes it vulnerable to physical and digital eavesdropping.

While data encryption during transmission provides a strong layer of security, the protection of endpoints often remains insufficient, leaving critical vulnerabilities unattended. Once data reaches its destination, such as a user's mobile phone, it is consumed in an unprotected or "cleartext" format, which allows it to be read directly from an adversary. If the device is not properly secured, attackers can easily intercept this unencrypted data, either through physical access (e.g. shoulder surfing) or digital means like malware or data breaches. Without proper endpoint protection, such as advanced encryption or secure storage mechanisms, sensitive information like passwords, financial details, and personal messages can be accessed by unauthorized parties [25].

Cleartext consumption of data on devices significantly increases the risks of both physical and digital eavesdropping. For instance, if a device is lost or stolen, an attacker could gain immediate access to valuable information that would otherwise be protected if encrypted. Similarly, through techniques like man-in-the-middle attacks or malware, digital eavesdropping can capture data as it is being processed on the device. These risks highlight the need for a comprehensive security strategy that includes robust encryption both in transit and at rest and endpoint protections to ensure that data remains secure throughout its entire lifecycle. Moreover, even if the user has installed all security features that could increase the protection of data, improper use of those or even bypass of them due to increased complexity or delay can expose private data to adversaries [26].

3.3 Client-Side Scanning (CSS)

E2E protocols have weakened the efficiency of Server-Side Scanning techniques. Proposed as a method to balance privacy and security, Client-Side Scanning (CSS) has raised a significant debate due to the new risks it introduces. CSS involves scanning users' data directly on users' devices to identify specific, targeted material, such as illegal content or potential threats. While the goal is to enhance security without compromising privacy, this approach creates a delicate balance. The idea of scanning users' data raises serious concerns about potential misuse, as it opens a backdoor for authorities, tech companies, or malicious actors to access personal information under the purpose of safeguarding peoples' security [27].

Furthermore, CSS could lead to false positives, where benign data is incorrectly flagged as a security threat or illegal content. This could result in unwarranted surveillance, censorship, or even legal consequences for individuals who aren't performing any illegal actions. Additionally, the implementation of CSS by governments or private entities raises concerns about overreach, with the possibility that such scanning could extend beyond its intended scope, violating civil liberties. The introduction of this technology calls for careful consideration of its ethical implications, ensuring that the protection of individual privacy is not compromised in the name of security.

3.4 Encryption Backdoors

Encryption is a dual-purpose technology that safeguards both the security of law-abiding individuals and the activities of criminals who use it to conceal evidence of their criminal activities. Likewise, encryption backdoors can serve dual purposes—while they

allow law enforcement to access communication content, they can also be exploited by criminals to obtain information, enabling cybercrimes like extortion, theft, and fraud.

Many countries like the U.S, the U.K., and France among others, seem very interested in mandating encryption backdoors, tools that give governmental authorities access to encrypted communication. This request is coming mainly from law enforcement authorities but is followed by the risk of reducing the security level of the offered service if not implemented correctly as mentioned in [6], security researchers agree that when any backdoor is applied in an E2E encryption mechanism it effectively removes the E2E security and weakens the encryption protocol for all users of this specific service. Additionally, opponents of mandatory government backdoors argue that encryption is essential for safeguarding individuals from cybercriminals and securing communications. This protection is particularly important for journalists, political dissidents, human rights advocates, domestic violence survivors, and businesses, among others.

3.5 Quantum Computing and AI

Quantum computers and AI pose significant threats to end-to-end encryption (E2EE) due to their ability to undermine traditional cryptographic algorithms [28]. Current E2EE systems rely on encryption techniques like RSA, ECC, and Diffie-Hellman, which derive their security from the difficulty of factoring large numbers or solving discrete logarithm problems. Quantum computers can solve these problems exponentially faster than classical computers, making these encryption methods obsolete. This would allow adversaries with quantum capabilities to decrypt previously secure communications. For that reason, A set of encryption algorithms that are designed to withstand hacking attempts by a quantum computer has been released by the US National Institute of Standards and Technology [29].

Meanwhile, AI increases the risks against security and privacy by enhancing the efficiency of cryptographic attacks, automating pattern recognition, and improving the exploitation of vulnerabilities in encryption protocols. Combined, quantum computing and AI could enable large-scale interception and decryption of sensitive communications, severely compromising privacy, financial security, and data protection. This evolving threat underscores the urgent need for post-quantum cryptography to secure E2EE systems against future adversarial advancements [30].

3.6 Ethical Implications

E2E encryption can offer enhanced data privacy protection but on other hand it can also be used for criminal activities. There was a recent example of EncroChat. EncroChat was a Europe-based communications network and service provider that offered modified smartphones enabling encrypted communication among subscribers. While initially marketed as a privacy-focused service, it became a vehicle for organized crime, facilitating activities such as drug trafficking and money laundering EncroChat was a Europe-based communications network and service provider that offered modified smartphones allowing encrypted communication among subscribers. It was used primarily by organized crime members to plan criminal activities. In early 2020, law enforcement agencies,

from France and the Netherlands, infiltrated EncroChat's encrypted network. This operation allowed them to monitor communications in real-time, leading to the arrestment of hundreds of suspects and the seize of substantial quantities of drugs, firearms, and cash [31].

4 Innovative E2E Mechanisms

In this section we briefly present recent innovative solutions that can be applied to add another layer of encryption, reassuring the privacy of user data.

4.1 The SNE2EE Framework

Recently we presented the secure node end to end (SNE2EE) mechanism. SNE2EE aims to extend encryption to the endpoints, addressing vulnerabilities overlooked by traditional E2E encryption [32] solutions. This innovative solution integrates hardware and software technologies to enhance security without compromising the usability of the end device [33].

Key Features of SNE2EE:

- End-Node Encryption: Data is encrypted in an external device before being transmitted to the user's mobile phone, ensuring protection of data at endpoints.
- Multifactor Authentication (MFA) mechanism: Enhanced user identity verification through methods like fingerprint recognition or RFID identification.
- External Hardware Integration: Devices like Raspberry Pi smart overlay screen, clean mobile phones or smart AR glasses create, encrypt, and display data, decoupling sensitive operations from vulnerable mobile devices.

SNE2EE encrypts cleartext messages using public-private key pairs that are created by the application or the user himself. The encrypted data is transmitted and further encrypted by host applications (any internet communication organisers (ICOs)), ensuring additional layer protection. Upon reception, the process is reversed, and the message is securely displayed via external hardware to the end user.

The SNE2EE prototype employs a Raspberry Pi, an external LCD screen, and an RFID device mainly used for identity verification. It demonstrates how hardware and software can synergize to mitigate risks from malware and stalkerware but it is not so user-friendly [12]. The second prototype demanded the use of a second'clear' mobile phone that the user would use for creating and consuming the messages [32]. SNE2EE third implementation included 2 pairs of AR glasses that can communicate through a messaging application and can perform several actions: speech-to-text transformation, encryption of text, sending of message, decryption of text, and overlay text display. This promising framework of E2E solutions can offer enhanced data privacy and can mitigate many vulnerabilities of existing solutions although adding complexity and cost to the end users.

The SNE2EE framework has broad applications, meeting security requirements across various sectors:

- Military and Law Enforcement: SNE2EE offers a highly secure communication channel, ensuring the confidentiality and integrity of sensitive operations.
- Industry Applications: Professionals in key sectors, particularly executives, gain protection from eavesdropping and data breaches.
- Individual Users: SNE2EE secures personal communications against malware, social media account takeovers, and financial fraud, fostering trust in digital platforms.

4.2 Encrypted Keyboard

Several encrypted keyboard applications, such as Enigma Encryption Keyboard [34] and WhisperKeyboard [35], are available on the Apple App Store and Google Play Store. These applications offer end-to-end encryption and decryption for text messages.

Moving one step further, the solution presented in [13] supports the encryption and decryption of not only text messages but also multimedia content such as images, audio, and video files. Designed as a system keyboard, the encrypted keyboard effectively mitigates the risk of CSS (Content Security System) technologies in many end-to-end encrypted systems. Once enabled as the primary keyboard on a user's phone, it seamlessly functions across all applications requiring user input, ensuring secure communication on every platform within the device. Additionally, the encrypted keyboard incorporates an automated decryption process. This eliminates the need for users to manually copy encrypted text to their phone's clipboard for decryption, as required by other applications. By streamlining this process, their approach reduces user effort and improves ease of use when decoding encrypted messages.

The SNE2EE framework and encrypted keyboard present promising solutions to enhance privacy and security in E2EE systems by mitigating CSS risks. While these innovations address critical concerns, improving usability, performance, and expanding compatibility will further strengthen its effectiveness and adoption.

5 Conclusions

E2E encryption is both a salvation and a challenge. It ensures privacy and security for billions but introduces complexities for law enforcement and policymakers. Solutions like SNE2EE offer a pathway to reconcile privacy with security, extending protection to endpoints without compromising functionality. Moving forward, collaboration among stakeholders—governments, technology providers, and privacy advocates—is essential. Only through dialogue and innovative approaches can we address the ethical, technical, and legal dilemmas of E2E encryption.

Acknowledgments. The authors would like to acknowledge the financial support provided for the following projects: The 'Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594; the 'Human-centered Trustworthiness Optimization in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101121042; the 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received

funding from the European Union's DEP programme under grant agreement No. 101127411; the 'A Certification approach for dynamic, agile and reUSable assessmenT fOr composite systems of ICT proDucts, servicEs, and processes' (CUSTODES) which has received funding from the European Union's Horizon Programme under grant agreement No. 101120684; the 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CyberSynchrony) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101158555; and the 'Fostering Artificial Intelligence Trust for Humans towards the Optimization of Trustworthiness through Large-scale Pilots in Critical Domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932. The views expressed in this paper represent only the views of the authors and not those of the European Commission or the partners in the above-mentioned projects. Finally, the authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts.

References

1. Losing digital trust will harm technological innovation: Here's how to earn it again. https://www.weforum.org/stories/2022/12/losing-digital-trust-will-harm-technological-innovation/
2. Endeley, R.E.: End-to-end Encryption, Backdoors, and Privacy. Capitol Technology University (2019)
3. The fbi wants you to stop texting without encryption. here's why. https://www.nbcboston.com/investigations/consumer/why-the-fbi-wants-you-to-stop-texting-without-encryption-heres-why/3571037/
4. Hartel, P., van Wegberg, R.: Going dark? Analysing the impact of end-to-end encryption on the outcome of dutch criminal court cases. Crime Sci. **12**(1), 5 (2023)
5. Joint declaration of the european police chiefs (2024). Accessed 1 Dec 2024. https://www.europol.europa.eu/media-press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end-to-end-encryption-roll-out
6. Shurson, J.: A European right to end-to-end encryption? Comput. Law Secur. Rev. **55**, 106063 (2024)
7. Sayjari, T., Silveira, R.M.: Ethics of privacy in cybersecurity: Protecting individual autonomy through technology (2024)
8. Kioskli, K., Maglaras, L., Fotis, T., Varouchas, E.: Human factors and strategic approaches in cybersecurity: threats for critical infrastructures in nis2 domains. In: AHFE International Conference on Human Factors in Design, Engineering, and Computing (2025)
9. Evans, M., Maglaras, L.A., He, Y., Janicke, H.: Human behaviour as an aspect of cybersecurity assurance. Secur. Commun. Netw. **9**(17), 4667–4679 (2016)
10. Isobe, T., Ito, R.: Security analysis of end-to-end encryption for zoom meetings. IEEE Access **9**, 90677–90689 (2021)
11. Nabeel, M.: The many faces of end-to-end encryption and their security analysis. In: 2017 IEEE International Conference on Edge Computing (EDGE) , pp. 252–259. IEEE (2017)
12. Maglaras, L., Ayres, N., Moschoyiannis, S., Tassiulas, L.: The end of eavesdropping attacks through the use of advanced end to end encryption mechanisms. In: IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) , pp. 1–2. IEEE (2022)
13. Alatawi, M., Saxena, N.: Exploring encrypted keyboards to defeat client-side scanning in end-to-end encryption systems. In: International Conference on Information Security and Cryptology, pp. 100–123. Springer, Heidelberg (2022)

14. Babaghayou, M., Chaib, N., Lagraa, N., Ferrag, M.A., Maglaras, L.: A safetyaware location privacy-preserving iov scheme with road congestion-estimation in mobile edge computing. Sensors **23**(1), 531 (2023)
15. Ullah, I., Shah, M.A.: SGO: semantic group obfuscation for location-based services in vanets. Sensors **24**(4), 1145 (2024)
16. Rad, P., Dorai, G., Jozani, M.: From seaweed to security: harnessing alginate to challenge iot fingerprint authentication. In: Proceedings of the 19th International Conference on Availability, Reliability and Security, pp. 1–10 (2024)
17. Wagner, I.: Privacy policies across the ages: content of privacy policies 1996–2021. ACM Trans. Priv. Secur. **26**(3), 1–32 (2023)
18. Englehardt, S., et al.: Cookies that give you away: the surveillance implications of web tracking. In: Proceedings of the 24th International Conference on World Wide Web, pp. 289–299 (2015)
19. Zard, L.: Consumer manipulation via online behavioral advertising. arXiv preprint arXiv:2401.00205 (2023)
20. Naef, T.: Data protection without data protectionism: the right to protection of personal data and data transfers in EU law and international trade law. Springer, Heidelberg (2023)
21. Hamza, R., Pradana, H.: A survey of intellectual property rights protection in big data applications. Algorithms **15**(11), 418 (2022)
22. Chowdhury, P.D., et al.: Threat models over space and time: a case study of e2ee messaging applications. arXiv preprint arXiv:2301.05653 (2023)
23. Enisa threat landscape. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
24. Gibson, C., et al.: Analyzing the monetization ecosystem of stalkerware. In: Proceedings on Privacy Enhancing Technologies (2022)
25. Nobles, C.: Stress, burnout, and security fatigue in cybersecurity: a human factors problem. Holistica–J. Bus. Public Administ. **13**, 49–72 (2022)
26. Karayel, T., Aktaş, B., Akbıyık, A.: Human factors in remote work: examining cyber hygiene practices Inf. Comput. Secur. (2024)
27. Abelson, H., et al.: Bugs in our pockets: the risks of client-side scanning. J. Cybersecur. **10**(1), tyad020 (2024)
28. Scholten, T.L., et al.: Assessing the benefits and risks of quantum computers. arXiv preprint arXiv:2401.16317 (2024)
29. Banks, M.: Nist publishes new encryption standards. Phys. World **37**(9), 11iii–11iii (2024). https://doi.org/10.1088/2058-7058/37/09/13
30. Aydeger, A., Zeydan, E., Yadav, A.K., Hemachandra, K.T., Liyanage, M.: Towards a quantum-resilient future: strategies for transitioning to post-quantum cryptography. In: 2024 15th International Conference on Network of the Future (NoF), pp. 195–203. IEEE (2024)
31. Stoykova, R.: Encrochat: the hacker with a warrant and fair trials? Forensic Sci. Int. Dig. Invest. **46**, 301602 (2023)
32. Velagala, N., Maglaras, L., Ayres, N., Moschoyiannis, S., Tassiulas, L.: Enhancing privacy of online chat apps utilising secure node end-to-end encryption (sne2ee). In: 2022 IEEE Symposium on Computers and Communications (ISCC), pp. 1–3. IEEE (2022)
33. Alsop, H., et al.: Arsecure: a novel end-to-end encryption messaging system using augmented reality. arXiv preprint arXiv:2409.04457 (2024)
34. Enigma encryption keyboard (2022). https://apps.apple.com/us/app/enigma-encryption-keyboard/id971945391?platform=iphone
35. Whisperkeyboard (2022). https://play.google.com/store/apps/details?id=cn.security.kbshrimp