A Survey of Privacy-Enhancing Technology: Case Study for Military Vehicle

Academic Article

Ukid Changsan[1] and Pongpisit Wuttidittachotti[2]
Department of Network and Information Security Management
Faculty of Information Technology and Digital Innovation
King Mongkut's University of Technology North Bangkok
E-mail: s6507031910018@email.kmutnb.ac.th[1] and pongpisit.w@itd.kmutnb.ac.th[2]

Abstract

Privacy-enhancing technologies (PETs) are instrumental tools, techniques, and practices aimed at safeguarding individuals' privacy by mitigating risks associated with data collection, storage, and processing. Their deployment extends to military contexts, where protection of sensitive information and operational security hold paramount importance. PETs enable military organizations to ensure the confidentiality, integrity, and availability of highly classified and sensitive data. Anonymity and pseudonymity technologies, data encryption and cryptography, privacy-enhancing communication protocols, trusted execution environments, privacy-focused web browsers and search engines, privacy-aware mobile applications, and blockchain-based PETs are some of the key types of PETs. These technologies deliver benefits such as privacy protection, data security, transparency, trust, compliance, and innovation. Two case studies exemplify the application of PETs: the first study analyzes a pseudonym-based approach to conceal the real identity of military vehicles, demonstrating superior time efficiency and secure communication, while the second study introduces the SecVLC protocol that addresses privacy and security concerns in visible light communication, promising enhanced security through directional transmission and secure key generation.

---

[1] Lieutenant, Army War College, Thailand

[2] Associate Professor Dr., Head of Department of Digital Network and Information Security Management, King Mongkut's University of Technology North Bangkok

วันที่รับบทความ: 31 พ.ค.66 วันที่แก้ไขบทความ: 19 มิ.ย.66 วันที่ตอบรับบทความ: 22 มิ.ย.66

Keywords: Privacy Enhancing Technologies, Personal information protection, Anonymity, Pseudonymity, Cryptography

Introduction

Privacy-enhancing technologies (PETs) (Information Commissioner's Office, 2022) are essential tools, techniques, and practices designed to safeguard individuals' privacy by protecting their personal data from unauthorized collection, storage, and processing. These technologies are not limited to civilian applications; they also hold significant relevance in military contexts where the protection of sensitive information and operational security are paramount. In addition to their relevance in civilian contexts, PETs hold significant importance in military environments where the protection of sensitive information and the preservation of operational security are paramount. Military organizations frequently handle highly classified and confidential data, necessitating the utilization of PETs to ensure the utmost confidentiality, integrity, and availability of this critical information. In addition to their relevance in civilian contexts, PETs hold significant importance in military environments where the protection of sensitive information and the preservation of operational security are paramount. Military organizations frequently handle highly classified and confidential data, necessitating the utilization of PETs to ensure the utmost confidentiality, integrity, and availability of this critical information. The adoption of PETs in military operations yields numerous benefits. Beyond safeguarding privacy, these technologies enhance data security, foster transparency, cultivate trust among stakeholders, ensure compliance with privacy regulations, and even stimulate innovation within the military domain.

To illustrate the practical application of PETs in military scenarios, two case studies are examined. The first case study centers on a pseudonym-based approach employed to protect the real identities of military vehicles. This innovative security scheme ensures location privacy through the implementation of novel pseudonym assignment and encryption schemes. By seamlessly concealing the original identity of each military vehicle, this approach facilitates secure communication, while simultaneously providing robust defenses against diverse forms of attacks. The second case study addresses privacy and security concerns inherent in visible light communication (VLC) utilized in military convoy formations. Leveraging the directional capabilities and secure key generation mechanisms of VLC, the SecVLC protocol ensures enhanced privacy and security, offering a reliable communication alternative to traditional radio frequency methods.

Types of Privacy-Enhancing Technologies

1. Anonymity and pseudonymity technologies

Anonymity and pseudonymity technologies are a subset of privacy-enhancing technologies (PETs) that are designed to protect users' identities and personal information online. Anonymity refers to the state of being unknown or unidentifiable, while pseudonymity refers to the use of a false name or identifier as figure 1.

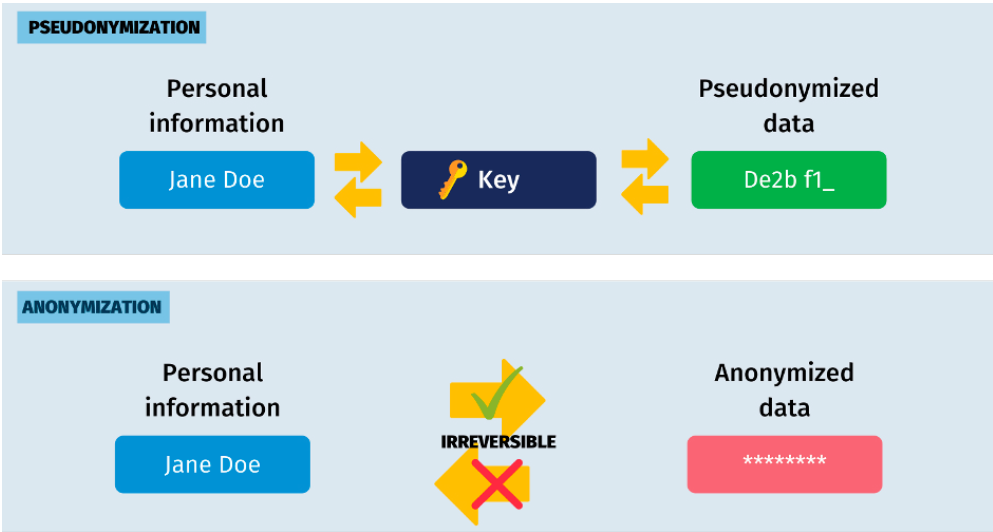


Figure 1 The difference between privacy protection Pseudonymization and Anonymization
Source: Locky, n.d.

Anonymity (Sardá, Natale, Sotirakopoulos, & Monaghan, 2019) technologies include tools like Tor, I2P, and Freenet, which allow users to browse the web and communicate online without revealing their IP address or location. These tools work by routing a user's internet traffic through a network of volunteer-run servers, making it difficult to trace their online activities back to their physical location. This can be particularly important for individuals living in countries with oppressive governments or those who wish to protect their privacy from corporations or other entities.

Pseudonymity technologies include tools like pseudonymous social media accounts, anonymous email services, and virtual private networks (VPNs). These tools allow users to create a false identity or use a pseudonym when communicating online, which can help to protect their privacy and prevent them from being targeted by malicious actors. However, it is important to note that pseudonymity is not always a guarantee of privacy, as it can be possible to link pseudonymous accounts to real-world identities through various means such as tracking online behavior or analyzing metadata.

While anonymity and pseudonymity technologies can be valuable tools for protecting online privacy, they can also be misused for illegal activities such as cyberbullying, harassment, and other malicious behavior. Therefore, it is important to use these technologies responsibly and to consider the potential impact on others when using anonymous or pseudonymous accounts. (Sucasas, Mantas, Bastos, Damiao, & Rodriguez, 2019) has presented research on case crowd detection requires authentication to maintain privacy. This allows users to anonymously submit detection reports in Smart City environments as shown in Figure 2.

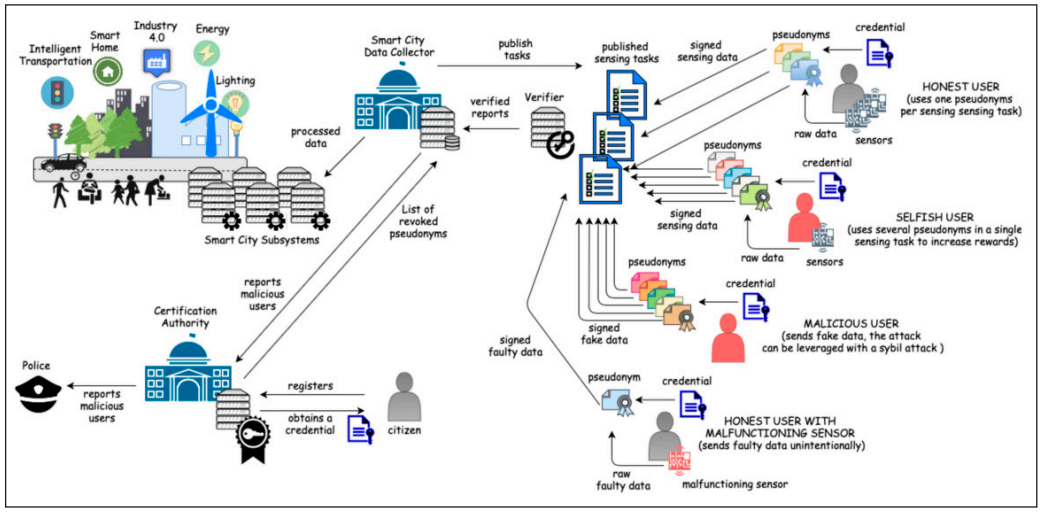


Figure 2: System model for the proposed pseudonym-based signature scheme

Source: Sucasas, Mantas, Bastos, Damiao, and Rodriguez, 2019

2. Data encryption and cryptography

Data encryption and cryptography are key privacy-enhancing technologies (PETs) used to protect sensitive information from unauthorized access or interception. Data encryption involves the use of algorithms to transform plaintext (unencrypted) data into ciphertext (encrypted) data. Cryptography (Akande, Abikoye, Kayode, Aro, & Ogandokun, 2020) refers to the science of encrypting and decrypting data, as well as designing and analyzing the security of encryption algorithms.

There are two primary types of encryptions: symmetric encryption and asymmetric encryption. In symmetric encryption, the same key is used to encrypt and decrypt the data. This type of encryption is commonly used for data that does not need to be shared between multiple parties. In asymmetric encryption, two keys are used- a public key and a private key- with the public key used to encrypt data and the private key used to decrypt data. This type of encryption is commonly used for secure communication between multiple parties.

Cryptography plays a critical role in ensuring the security of encrypted data. Cryptographic techniques such as hash functions, digital signatures, and message authentication codes (MACs) are used to verify the authenticity and integrity of encrypted data. Hash functions, for example, are used to generate a unique fixed-length string of characters (hash) from a given input. This hash can be used to verify the integrity of the data by comparing the hash of the original data to the hash of the encrypted data. Digital signatures are used to provide non-repudiation, meaning that the sender of a message cannot later deny having sent it.

3. Privacy-enhancing communication protocols

Privacy-enhancing communication protocols (Makin, & Ireland, 2020) are a set of techniques and protocols designed to protect the privacy and security of communications over digital networks. These protocols aim to ensure that sensitive information such as personal data, financial information, and other confidential data remain private and secure during communication.

One example of Privacy-enhancing communication protocols is the use of secure communication channels such as virtual private networks (VPNs) and secure sockets layer (SSL) protocols. These protocols ensure that data is encrypted during transmission, making it difficult for unauthorized parties to intercept and read the data. This is particularly important in situations where sensitive data needs to be transmitted over public networks such as the Internet.

Another example of Privacy-enhancing communication protocols is the use of anonymity networks such as Tor. Anonymity networks allow users to communicate anonymously over the Internet, making it difficult for third parties to trace the communications back to specific individuals or organizations. This can be useful in situations where users want to protect their identity or avoid surveillance.

4. Trusted execution environments and secure enclaves

Trusted execution environments (TEEs) and secure enclaves are hardware-based security features designed to protect sensitive data and computations from unauthorized access. These technologies are particularly useful in situations where sensitive data needs to be processed on untrusted devices, such as in cloud computing environments.

A TEE is a secure area of a processor that is isolated from the main operating system and provides a secure environment for executing sensitive code and data. A TEE provides a trusted environment for executing code and data, preventing attacks such as code injection and tampering. TEEs typically provide hardware-based isolation, ensuring that sensitive data and computations are kept separate from other applications and processes on the device.

Secure enclaves are a similar technology used in Apple devices, known as the Secure Enclave. The Secure Enclave isa hardware-based security feature that provides a separate processing environment within the device's CPU. It is used to store sensitive data such as biometric information, passwords, and encryption keys, as well as for performing sensitive computations such as encryption and decryption. The Secure Enclave is isolated from the main operating system and other applications running on the device, ensuring that sensitive data and computations are protected from unauthorized access.

Table: Company have trusted execution environments and secure enclaves.

Company	Product	Hardware Used	References
Alibaba	Cloud Link TEE		(Alibaba Tech, 2019)
Apple	iOS Secure Enclave	Separate processor	(Apple Platform Security, 2021)
BeanPod		Arm TrustZone	(GlobalPlatform, 2016)
Huawei	iTrustee	Arm TrustZone	(Huawei, 2019)
Google	Trusty	ARM / Intel	(Android Open Source Project, 2021)
Linaro	OPTEE	Arm TrustZone	(Linaro, 2021)
Qualcomm	QTEE	ARM TrustZone	(Qualcomm,2021)
Samsung	TEEgris	Arm TrustZone	(GlobalPlatform ,2020)
Watchdata	WatchTrust	Arm TrustZone	(GlobalPlatform ,2018)

Both TEEs and secure enclaves use hardware-based security features to protect sensitive data and computations from unauthorized access. These technologies provide a secure environment for executing sensitive code and data, preventing attacks such as code injection and tampering. They are particularly useful in situations where sensitive data needs to be processed on untrusted devices, such as in cloud computing environments.

5. Privacy-focused web browsers and search engines

Privacy-focused web browsers and search engines are software applications designed to protect (Borgolte & Feamster, 2020) the privacy and security of user data while browsing the internet. These tools are designed to minimize the collection and sharing of user data by websites and online services, and to provide users with greater control over their personal information.Privacy-focused web

browsers typically include features such as ad blockers, anti-tracking technology, and secure connections using HTTPS. Ad blockers prevent advertisements from loading on websites, which can reduce the amount of data collected by advertisers and third-party trackers. Anti-tracking technology prevents online services from collecting data about user behavior, such as browsing history and search queries. Secure connections using HTTPS encrypt user data during transmission, preventing eavesdropping and data interception.

Examples of privacy-focused web browsers include Brave, Mozilla Firefox, and Tor. These browsers are designed to protect user privacy by minimizing the collection of data and providing users with greater control over their personal information.

6. Privacy-aware mobile applications

Privacy-aware mobile applications are software applications designed to protect the Privacy and security of user data on mobile devices. These applications are developed with a focus on minimizing the collection and sharing of user data, and providing users with greater control over their personal information.

Mobile applications (Xiong, Li, He, Liu, & Peng, 2022) can collect a wide range of user data, including location data, contacts, browsing history, and personal preferences. Privacy-aware mobile applications must be designed to minimize the collection of this data, and to provide users with greater control over how their data is used.

Privacy-aware mobile applications encompass a range of features that contribute to enhancing user privacy and security. These applications may offer functionalities such as the ability to opt-out of data collection, data encryption during transmission, and options to delete or export user data. Additionally, they prioritize transparency by providing users with clear and concise privacy policies. Privacy-enhancing technologies, such as data anony-mization and pseudonymization, may also be implemented to bolster user privacy. The significance of privacy-aware mobile applications is heightened due to the increasing reliance on mobile devices for sensitive activities like online banking and healthcare. Furthermore, as mobile devices are commonly used in public settings, they become susceptible to theft and unauthorized access. Prominent examples of privacy-aware mobile applications include Signal, a messaging platform that employs end-to-end encryption to safeguard user data, and ProtonMail, an email service that upholds end-to-end encryption and refrains from collecting user data for advertising purposes. These applications serve as noteworthy illustrations of how privacy-aware practices can be implemented in mobile applications to protect user privacy and maintain data security.

7. Blockchain-based PETs

Blockchain-based Privacy Enhancing Technologies (PETs) are a relatively new development (Javed, Alharbi, Margaria, Crespi, & Qureshi, 2021) that aims to provide users with a higher level of privacy and security for their online transactions and interactions. Blockchain technology is a distributed ledger system that uses cryptographic techniques to ensure the immutability and security of data stored in the ledger. One of the primary applications of blockchain-based PETs is in the area of identity management. Blockchain technology offers the potential to establish self-sovereign identities (SSI) that are decentralized and under the control of individual users. This decentralized nature enables users to retain authority over their personal data and exercise control over the extent of information disclosed to third parties. By leveraging blockchain, users can establish a framework that prioritizes privacy and empowers individuals to safeguard their personal information in a secure and autonomous manner.

Blockchain-based PETs can also be used to enhance the privacy and security of online transactions. By using blockchain technology, it is possible to create secure and verifiable transaction records that cannot be tampered with or altered. This can be particularly useful in situations where trust is an issue, such as in financial transactions or online voting. Another application of blockchain-based PETs is in the area of data privacy. By using blockchain technology to store and share data, it is possible to create a more secure and private data-sharing ecosystem. For example, sensitive medical data can be stored on a blockchain and only shared with authorized parties, providing patients with greater control over their personal information.

Blockchain-based PETs have the potential to provide users with a higher level of privacy and security for their online transactions and interactions. These technologies can be used for identity management, secure and verifiable transactions, and data privacy. However, there are also challenges to be addressed, particularly in terms of scalability and environmental impact.

Benefits of Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) have numerous benefits for protecting personal information and privacy rights in various contexts, including:

1. Privacy protection: PETs can help prevent unauthorized access, collection, and use of personal data, thereby safeguarding individuals' privacy rights.

2. Data security: By using encryption, access control mechanisms, and other security measures, PETs can protect sensitive data from cyber-attacks and data breaches.

3. Transparency: PETs can enable individuals to have more control over their personal data and to be aware of how it is being collected, used, and shared.

4. Trust: By implementing PETs, organizations can demonstrate their commitment to protecting personal data and respecting individuals' privacy rights, which can help build trust with their stakeholders.

5. Compliance: PETs can help organizations comply with privacy regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and Personal Data Protection Act (PDPA) of Thailand.

6. Innovation: By allowing individuals to share their personal data in a privacy-preserving way, PETs can enable the development of new services and applications that rely on personal data, such as healthcare, finance, and marketing.

Overall, PETs can help individuals and organizations balance the benefits of using personal data with the need to protect privacy and maintain trust. By implementing PETs, organizations can demonstrate their commitment to protecting personal data and respecting individuals' privacy rights.

Case Study1: In the study conducted by (Tandon & Gupta, 2021), a comprehensive analysis was performed on a pseudonym-based approach to protect the real identity of military vehicles. The main objective of the study was to ensure the location privacy of these vehicles through the implementation of novel pseudonym assignment and encryption schemes. The proposed security scheme utilized a hybrid approach, combining the matrix array symmetric key and the intelligent water drop scheme. By adopting this security scheme, each military vehicle could obtain a pseudonym, effectively concealing its original identity. The proposed algorithm efficiently managed pseudonym generation and change requests in both local and inter-region environments. Moreover, the security scheme not only facilitated secure communication and preserved the location privacy of military vehicles but also provided defense against various forms of attacks. The study's comprehensive analysis demonstrated that the proposed algorithms exhibited superior time efficiency compared to existing techniques, both in local and inter-region scenarios.

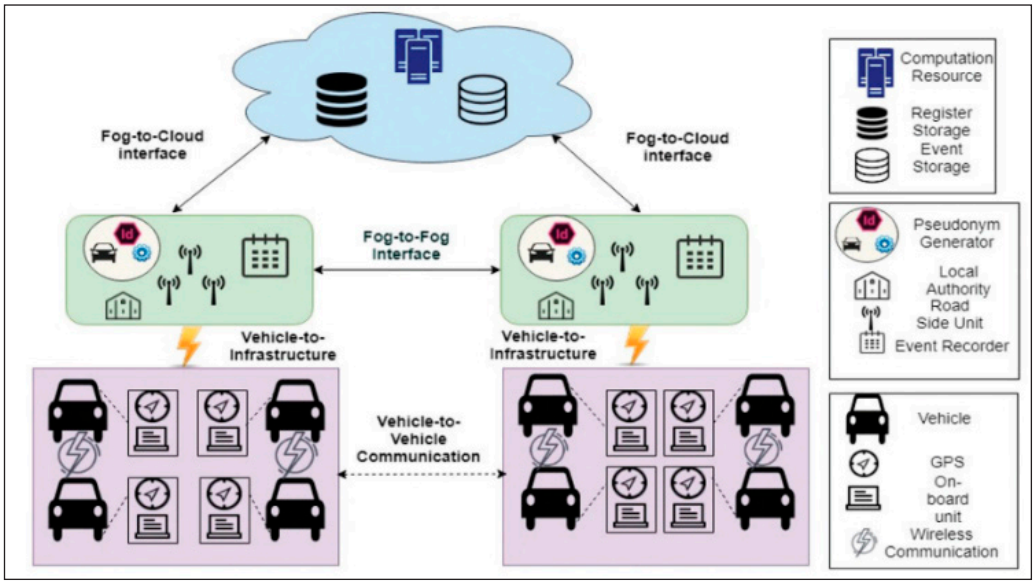


Figure 3: Proposed vehicle to vehicle communication framework

Source: Tandon and Gupta, 2021

In figure 3 illustrates the framework of the case study, which consists of three layers: the user layer, the fog layer, and the cloud layer.

Cast study 2: In a case study conducted by S. (Ucar, Ergen, Ozkasap, Tsonev, & Burchardt, 2016), a new protocol called Secure Visible Light Communication (SecVLC) was proposed as a relevant Privacy-Enhancing Technology. The protocol consists of 3 steps:

1. Utilizing the directionality property of Visible Light Communication (VLC) to ensure that only the intended vehicles participate in the communication. This ensures that the communication remains private and secure.

2. Implementing full-duplex communication, where infrared (IR) serves as the outgoing link to share a secret key, and VLC serves as the incoming link to receive encrypted vehicle data. This approach allows for simultaneous transmission and reception, enhancing the efficiency and effectiveness of secure communication.

3. Operating with a key generation and sharing mechanism that is crucial for data encryption and decryption. The protocol generates and shares unique keys that are utilized to encrypt and decrypt data packets. This ensures that data remains confidential and cannot be decrypted without the corresponding generated keys.

The SecVLC protocol addresses the privacy and security concerns associated with visible light communication by leveraging its directional capabilities, full-duplex communication, and secure key generation and sharing mechanisms.

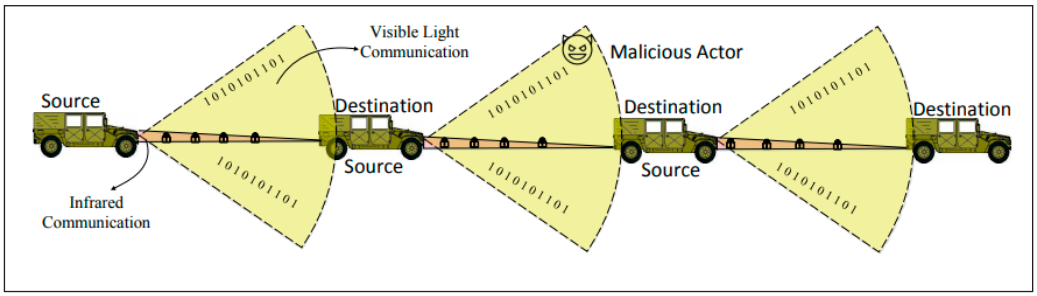


Figure 4: System model for the vehicular ad hoc network military

Source: Ucar, Ergen, Ozkasap, Tsonev, and Burchardt, 2016

In Figure 4, the integration of vehicular ad hoc network (VANET) with Intelligent Transportation System (ITS) and Intelligent Traffic System (ITF) is depicted. Within this context, VANET serves as a crucial component for facilitating secure and reliable communication, particularly in military applications where vehicles operate in a convoy formation. Traditional radio frequency (RF) communication, commonly used in VANET, presents limitations in military scenarios due to the scarcity of available frequency bands and its vulnerability to security attacks. As a promising alternative, Visible Light Communication (VLC) has emerged, offering enhanced security by restricting the reception of neighboring nodes through directional transmission.

Conclusion

Privacy-enhancing technologies (PETs) play a critical role in safeguarding individuals' privacy and have significant relevance in both civilian and military contexts. In civilian applications, PETs protect personal data from unauthorized collection, storage, and processing. Similarly, in military environments, PETs are essential for ensuring the confidentiality, integrity, and availability of highly classified and confidential information. The adoption of PETs in military operations brings various benefits, including enhanced data security, transparency, trust, compliance with privacy regulations, and fostering innovation. Two case studies demonstrate the practical application of PETs in military scenarios, highlighting the effectiveness of pseudonym-based approaches in protecting the identities of military vehicles and the use of Secure Visible Light Communication (SecVLC) to enhance privacy and security in convoy formations. Overall, the utilization of PETs in both civilian and military contexts is vital for preserving privacy and securing sensitive information in today's digital age.

Finally, Implementing PETs demonstrates an organization's commitment to protecting personal data and respecting privacy rights, fostering trust with stakehold ers. By complying with privacy regulations such as the GDPR, CCPA, and PDPA, organizations can ensure legal compliance and uphold privacy standards.

References

Alibaba Tech. (2019). *Alibaba.* Retrieved form https://102.alibaba.com/detail/?id=367&mtime=1563847710000

Akande, O. N., Abikoye, O. C., Kayode, A. A., Aro, O. T., & Ogundokun, O. R. (2020). A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security. In Gervasi, O., Murgante, B., Misra, S., Garau, C., Blečić, I., Taniar, D., ..., Karaca, Y. (Eds.), *Proceeding Computational Science and Its Applications-ICCSA 2020 (487-499).* Retrieved form https://doi.org/10.1007/978-3-030-58817-5_36

Android Open Source Project. (2021). *Trusty TEE.* Retrieved form https://source.android.com/docs/security/features/trusty

Apple Platform Security. (2021). *Secure Enclave.* Retrieved form https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web

Borgolte, K. & Feamster, N. (2020). Understanding the Performance Costs and Benefits of Privacy-focused Browser Extensions. In Huang, Y., King, I., Liu, T. Y., Steen, M. V. (Eds.), *WWW '20: Proceedings of The Web Conference 2020 (2275-2286).* Retrieved form https://doi.org/10.1145/3366423.3380292

GlobalPlatform. (2016). *GlobalPlatform Welcomes New Participating Member Beijing Beanpod Technology.* Retrieved form https://globalplatform.org/latest-news/globalplatform-welcomes-new-participating-member-beijing-beanpod-technology/

_____. (2018). *WatchTrust 2.1.1 on SC9860.* Retrieved form https://globalplatform.org/wp-content/uploads/2018/09/GP-TEE-2018_01-CR-1.0_GP170003-Certificate-Certification-Report_20180904-signed-1.pdf

_____. (2020). *Samsung TEEgris v4.1 on Exynos 990/980 devices.* Retrieved form https://globalplatform.org/wp-content/uploads/2020/10/GP-TEE-2020_01-CR-1.0_GP200007-Certificate-and-Certification-Report_20200922.pdf

Huawei. (2019). *HUAWEI Privacy.* Retrieved form https://consumer.huawei.com/en/privacy/certification/

Information Commissioner's Office. (2022). *Privacy-enhancing technologies (PETs).* Retrieved form https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

Javed, I. T., Alharbi, F., Margaria, T., Crespi, N. & Qureshi, K. N. (2021). PETchain: A Blockchain-Based Privacy Enhancing Technology. *IEEE Access, 9,* Retrieved form https://doi.org/10.1109/ACCESS.2021.3064896

Linaro. (2021). *Trustzone and OP-TEE.* Retrieved form https://www.linaro.org/services/security/

Lockey, T. (n.d.). *Top Ten Privacy Enhancing Technologies.* Retrieved form https://www.techyv.com/article/top-ten-privacy-enhancing-technologies/

Makin, D.A. & Ireland, L. (2020). The secret life of PETs: A cross-sectional analysis of interest in privacy enhancing technologies. *Policing: An International Journal, 43*(1), Retrieved form https://doi.org/10.1108/PIJPSM-07-2019-0124

Qualcomm. (2021). *Guard your Data with Qualcomm Snapdragon Mobile Platform.* Retrieved form https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/guard_your_data_with_the_qualcomm_snapdragon_mobile_platform2.pdf

Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019). Understanding online

Anonymity. Media, Culture & Society, 41(4), Retrieved form https://doi.org/10.1177/0163443719842074

Sucasas, V., Mantas, G., Bastos, J., Damião, F., & Rodriguez, J. (2019). A Signature Scheme with Unlinkable-yet-Accountable Pseudonymity for Privacy-Preserving Crowdsensing. *IEEE Transactions on Mobile Computing, 19*(20), Retrieved form https://dl.acm.org/doi/10.1109/TMC.2019.2901463

Tandon, R., & Gupta, P. K. (2021). A Novel Pseudonym Assignment and Encryption Scheme for Preserving the Privacy of Military Vehicles. *Defence Science Journal, 71*(2), Retrieved form https://doi.org/10.14429/dsj.71.15534

Ucar, S., Ergen, S. C , Ozkasap, O., Tsonev, D., & Burchardt, H. (2016). SecVLC: Secure Visible Light Communication for Military Vehicular Networks. In Cuevas, A., Chatzimisios, P., & Grande, R. D. (Eds.), MobiWac '16: Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access (123-129). Retrieved form https://doi.org/ 10.1145/2989250.2989259

Xiong, L., Li, F., He, M., Liu, Z. & Peng, T. (2020). An Efficient Privacy-Aware Authentication Scheme With Hierarchical Access Control for Mobile Cloud Computing Services. *IEEE Transactions on Cloud Computing, (10)*4, Retrieved form https://doi.org/10.1109/TCC.2020.3029878