SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A++’ Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECE306- SMART IoT APPLICATIONS

III ECE / V SEMESTER

UNIT 5 – IOT LEGAL PERSPECTIVES AND STANDARDIZATION

TOPIC 2 –Security and Privacy: Privacy Enhancing Technologies

Privacy Enhancing Technologies (PET)

- Privacy Enhancing Technologies (PET) aim **to increase privacy** by implementing technological measures across various levels of interaction, including subject, object, transaction, and system orientations.
- These technologies help **users protect their personal data**, secure their identities, and anonymize their online transactions and interactions.

Privacy Enhancing Technologies (PET)

PETs are diverse and target different aspects of information privacy. There are four main orientations of PET:

Subject-oriented PET: Aims to limit the discernibility of a user's identity by others.

Object-oriented PET: Utilizes specific technologies to protect identities.

Transaction-oriented PET: Focuses on safeguarding transactional data, often through automated data destruction systems.

System-oriented PET: Creates interaction zones where users remain anonymous, and objects do not retain identifiable traces

Privacy Enhancing Technologies (PET)

- A fifth category, the Platform for Privacy Preferences (P3P), is under development by the World Wide Web Consortium (W3C).
- This aims **to allow users to program their browsers to control the information they share with websites**. However, P3P is not yet operational, and its effectiveness is uncertain.
- Additionally, a **Public Key Infrastructure (PKI)**-like system for data authentication is proposed to meet user privacy requirements, though it faces challenges such as potential identification of tagged objects by authenticated users and security vulnerabilities in communication channels.

Specific Technical Measures

1. Virtual Private Networks (VPN)

VPNs **create secure extranets for closed groups**, enhancing confidentiality among partners. However, they are limited in scalability and are impractical for third-party interactions beyond the extranet.

2. Transport Layer Security (TLS)

TLS enhances confidentiality and integrity in IoT communications but requires new connections for each delegation step, which can hinder information retrieval efficiency.

Specific Technical Measures

3. DNS Security Extensions (DNSSEC)

DNSSEC employs public-key cryptography to ensure data integrity and authenticity but does not address confidentiality. Its adoption is limited due to scalability issues and trust management challenges.

4. Onion Routing

Onion routing encrypts data in multiple layers to obscure the source of Internet traffic. While it enhances anonymity, it may degrade performance and does not guarantee data confidentiality or integrity.

Specific Technical Measures

5. Private Information Retrieval (PIR)

PIR systems aim to conceal user queries in globally accessible systems like ONS but face scalability and performance challenges that hinder practical implementation.

6. Peer-to-Peer Systems (P2P)

P2P systems facilitate decentralized data exchange among equal participants. They offer scalability and anonymity through encryption but require robust access controls to prevent misuse.

Specific Technical Measures

7. Switching off RFID Tags

Disabling RFID tags can be achieved through methods like using a Faraday Cage or issuing a "kill" command. However, both methods have drawbacks, such as the potential for reactivation or incomplete disabling of identifying information.

Specific Technical Measures

Conclusion

The landscape of Privacy Enhancing Technologies encompasses a variety of approaches aimed at protecting user privacy in digital interactions.

While each category presents unique advantages and challenges, ongoing developments in standards like P3P and technologies such as DNSSEC and TLS highlight the evolving nature of privacy concerns in an increasingly interconnected world.

Addressing these challenges will be crucial for enhancing user trust and ensuring effective privacy protection mechanisms across various digital platforms.