***MINI PROJECT ONE(1)***

**1970s: The Birth of Cybersecurity:** The term "computer security" was first coined as the need for securing data begins to emerge with the rise of mainframe computing. **APPARNET** and first known **computer virus** was introduced during this decade.

**1980s: Early Threats & Responses:** The introduction of internet worm and antivirus software to combat the internet worm occurred during this decade. The **Morris Worm**, one of the first major cybersecurity attacks on the early internet, causes significant damage, infecting around 10% of the internet.

**1990s: The Rise of Hacking & Encryption:**  The creation of Computer Emergency Response Team (CERT), Secure Sockets Layer (SSL) protocol to secure online transaction, and the first data breach when hackers access the credit card data of over 10million customers occurred during this decade.

**2000s: The Explosion of Cybercrime and Advanced Security Solutions:** The "ILOVEYOU" virus, a computer worm spread via email, becomes one of the most widespread and destructive attacks in history. The introduction of firewalls, Botnets and phishing attack was recorded. Estonian Government became the first major instances of politically motivated attacks.

**2010s: Advanced Persistent Threats (APTs) and Data Protection Legislation:** The Stuxnet worm was discovered, targeting Iran’s nuclear facilities. This marks the first known cyberattack on critical infrastructure, demonstrating the potential of cyber weapons.

Incidents like: Edward Snowden leaks classified information revealing extensive global surveillance by the NSA, raising awareness about privacy concerns and governmental overreach, the Sony Pictures hack was one of the most high-profile cyberattacks, allegedly carried out by North Korea, exposing the vulnerability of businesses to politically motivated cybercrime, the WannaCry ransomware attack spreads rapidly across the globe, affecting hundreds of thousands of computers, highlighting the dangers of unpatched vulnerabilities in outdated software were recorded in this decade.

The European Union enforces the GDPR, creating a stringent framework for data protection and privacy laws. This marks a major shift toward accountability in data handling.

**2020s: Ransomware Evolution, Zero-Trust Security, and AI Integration:** The concept of ransomware-as-a-service emerged, allowing cybercriminals with limited technical knowledge to launch ransomware attacks, exponentially increasing the scale of attacks.

The SolarWinds cyberattack compromises the supply chain of major global organizations, demonstrating the vulnerabilities in software supply chains and advanced persistent threat (APT) tactics. The concept of Zero-trust security models become mainstream, emphasizing the principle of "never trust, always verify," as organizations move towards more granular and robust security architectures in response to evolving threats.

**2025** (Projected): **AI and Quantum Computing in Cybersecurity:** AI is increasingly used for detecting anomalies, enhancing threat intelligence, and automating responses. The potential future integration of quantum computing is expected to revolutionize encryption and decryption techniques, posing both challenges and opportunities for the cybersecurity landscape.