6. Theory and Application of Zero Trust Security- A Brief Survey

NEED CITATION**

1. **Inadequacy of Traditional Perimeter-Based Security**: The paper highlights the increasing inadequacy of traditional perimeter-based network security models in coping with evolving security requirements, especially with the rise of cross-border access.
2. **Concept of Zero Trust**: Zero trust is introduced as a novel cybersecurity paradigm based on the core concept of "never trust, always verify," aiming to protect against both internal and external security risks by eliminating the traditional demarcations between internal and external networks.
3. **Emergence and Evolution of Zero Trust**: The paper discusses the origin, concepts, and principles of zero trust. It notes that zero trust is still a relatively new area of study, requiring more extensive research for deeper understanding in both academia and industry.
4. **Application in Cloud and IoT**: The characteristics, strengths, and weaknesses of existing research on zero trust are analyzed, particularly focusing on its technical applications in Cloud and IoT environments.
5. **Principles of Zero Trust Security by Kindervag**: The paper references the three principles for zero trust security proposed by John Kindervag, which include verifying and securing all sources, limiting and strictly controlling access, and inspecting and logging all network traffic.
6. **Development and Application of Zero Trust**: Zero trust has been developed in parallel with theoretical studies, particularly in cyber enterprises like Google, which implemented BeyondCorp, a zero-trust-based security method for internal networks.
7. **Exploration of Zero Trust Literature**: The paper conducts a systematic review of the literature on zero trust concepts, theory, achievements, and applications, aiming to provide a comprehensive understanding of zero trust. It also discusses the current challenges and future directions of zero trust, particularly from the perspective of trust itself in zero trust environments.

These key points emphasize the shift from traditional security models to the zero trust approach, its theoretical underpinnings, practical implementations, and the ongoing need for research and development in this area.