A trustworthy, reliable and lightweight privacy and data integrity approach for the internet of things

ABSTRACT

Data integrity and authenticity are among the key challenges faced by the interacting devices of Internet of Things (IoT). The resource-constrained nature of sensor-embedded devices make it even more difficult to design lightweight security schemes for these networks. In view of limited resources of the IoT devices, this paper proposes a lightweight and trustworthy device-to-server mutual authentication scheme for edge-enabled IoT networks. Initially, a trusted authority (TA) generates and assigns identities (IDs) and mask them to servers and clients, also known as member devices, in an off-line phase. These IDs are utilized to prevent possible infiltration of the adversary device(s). Next, every device ensures the authenticity of requesting devices using a sophisticated challenge, which is encrypted using a 128-bits secret key, λi. Each device expects a reply from the intended destination device for resolving the encrypted challenge within the defined time-frame, i.e.,△T. Moreover, authenticity of the requesting device is verified through the stored IDs which are shared in the off-line phase. Simulation results have verified the exceptional performance of the proposed authentication scheme against field proven approaches in terms of computational and communication costs, respectively.