Server Web pentru locuințe inteligente

Teodor

Rezumat

Internet of Things este un concept care se definește ca fiind o infrastructură globală pentru societatea informațională, dând posibilitatea de servicii avansate prin interconectarea, fizică sau virtuală, a lucrurilor bazate pe informația interoperațională existentă și în dezvoltare, iar pentru aceste scopuri, un "obiect" reprezintă un obiect al lumii fizice sau a lumii informațiilor, ce este capabil să fie identificat și integrat în rețele de comunicare. Pentru a stabili un grad de încredere între informția transmisă si cea recepționată, atât la nivelul comunicației dintre diversele componente cât și la nivelul comunicației cu utilizatorul final, sunt folosiți diverși algoritmi criptografici pentru securizarea comunicației și criptarea datelor.

Principala metodă de securizare a comunicației este reprezentată de utilizarea protocolului SSL (Secure Sockets Layer). SSL reprezintă o tehnologie standard de securitate pentru stabilirea unei legături criptate dintre un server și un client, de obicei un server web și un browser. Pentru a putea fi implementat un astfel de protocol, este necesară utilizarea unui pachet format dintr-o cheie publică și un certificat ce pot fi achiziționate de la autorități competente în acest sens, sau prin utilizarea bibliotecii OpenSSL, care generează aceste fișiere pe suportul flash al sistemului pe care este instalat server-ul. Deoarece aceste fișiere sunt stocate fizic, ele pot fi țința unor atacuri. Din acest motiv s-a trecut la o nouă metodă de securizare a informației folosind dispozitive TPM.

Un TPM (Trusted Platform Module) este un microcip conectat la placa de bază a unui computer. Scopul unui TPM este acela de genera si stoca chei criptografice, de exemplu chei RSA. Generând chei în mod hardware ce sunt stocate într-un dispozitiv din care acestea nu pot fi extrase, doar utilizate, un TPM reprezintă o soluție foarte eficientă pentru problema securizării datelor, fără a fi vulnerabil din exterior.

Această lucrare de diplomă își propune a demonstra conceptul de Internet of Things prin automatizarea și controlarea unor dispozitive de uz casnic prin intermediul unei pagini web. Vor fi prezentate principalele aspecte referitoare la SSL și certificatele folosite, structura generală a unui TPM, cheile folosite de acesta și modul în care un utilizator comunică direct cu un TPM. Pe baza acestor cunoștințe acumulate, vor fi implementate certificatele SSL pentru a realiza o comunicație securizată cu utilizatorul final, iar un TPM va fi folosit pentru a cripta și salva informația considerată utilă.