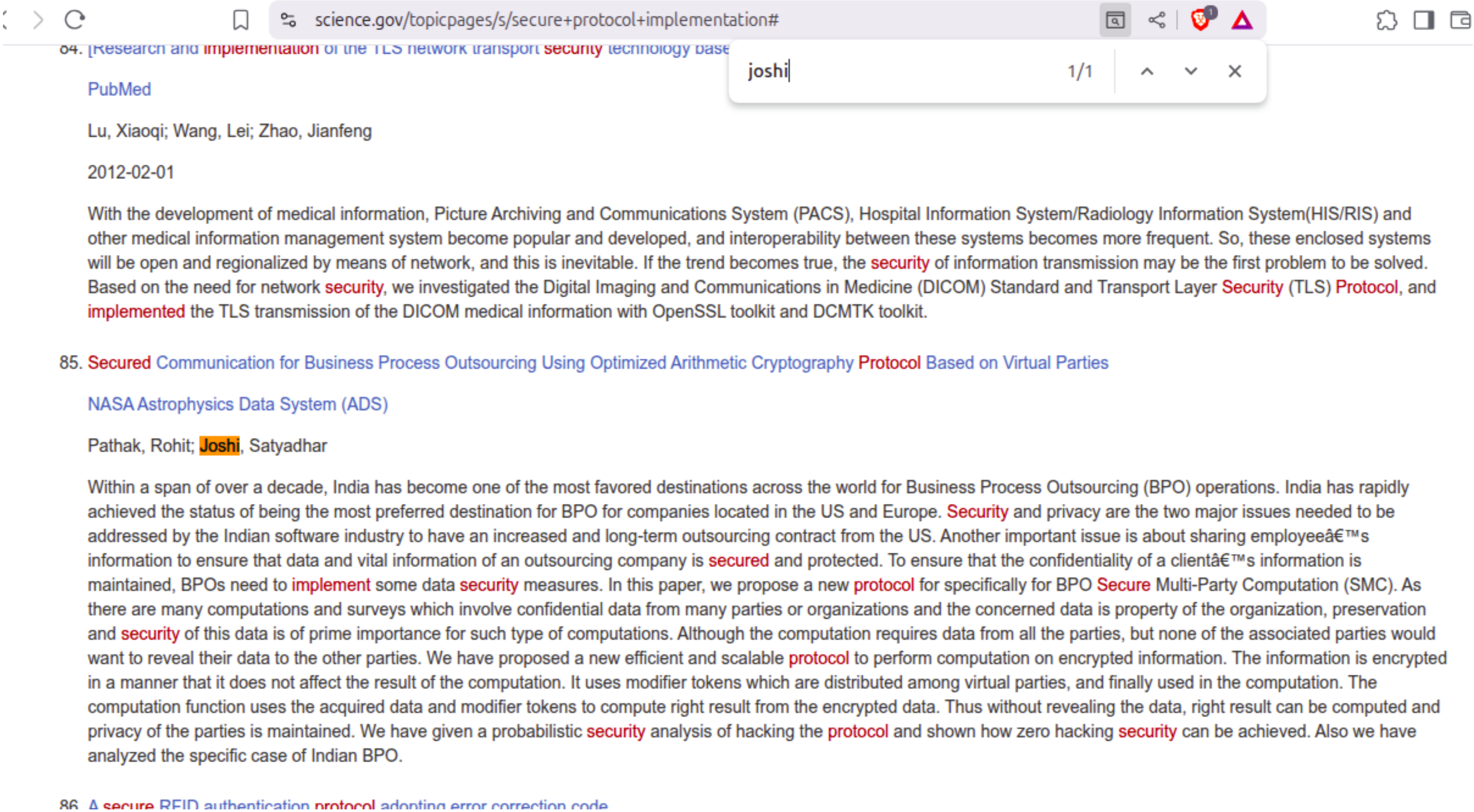

84. [Research and implementation of the TLS network transport security technology base

PubMed

Lu, Xiaoqi; Wang, Lei; Zhao, Jianfeng

2012-02-01

With the development of medical information, Picture Archiving and Communications System (PACS), Hospital Information System/Radiology Information System(HIS/RIS) and other medical information management system become popular and developed, and interoperability between these systems becomes more frequent. So, these enclosed systems will be open and regionalized by means of network, and this is inevitable. If the trend becomes true, the security of information transmission may be the first problem to be solved. Based on the need for network security, we investigated the Digital Imaging and Communications in Medicine (DICOM) Standard and Transport Layer Security (TLS) Protocol, and implemented the TLS transmission of the DICOM medical information with OpenSSL toolkit and DCMTK toolkit.

85. Secured Communication for Business Process Outsourcing Using Optimized Arithmetic Cryptography Protocol Based on Virtual Parties

NASA Astrophysics Data System (ADS)

Pathak, Rohit; Joshi, Satyadhar

Within a span of over a decade, India has become one of the most favored destinations across the world for Business Process Outsourcing (BPO) operations. India has rapidly achieved the status of being the most preferred destination for BPO for companies located in the US and Europe. Security and privacy are the two major issues needed to be addressed by the Indian software industry to have an increased and long-term outsourcing contract from the US. Another important issue is about sharing employeeâ€™s information to ensure that data and vital information of an outsourcing company is secured and protected. To ensure that the confidentiality of a clientâ€™s information is maintained, BPOs need to implement some data security measures. In this paper, we propose a new protocol for specifically for BPO Secure Multi-Party Computation (SMC). As there are many computations and surveys which involve confidential data from many parties or organizations and the concerned data is property of the organization, preservation and security of this data is of prime importance for such type of computations. Although the computation requires data from all the parties, but none of the associated parties would want to reveal their data to the other parties. We have proposed a new efficient and scalable protocol to perform computation on encrypted information. The information is encrypted in a manner that it does not affect the result of the computation. It uses modifier tokens which are distributed among virtual parties, and finally used in the computation. The computation function uses the acquired data and modifier tokens to compute right result from the encrypted data. Thus without revealing the data, right result can be computed and privacy of the parties is maintained. We have given a probabilistic security analysis of hacking the protocol and shown how zero hacking security can be achieved. Also we have analyzed the specific case of Indian BPO.

86. A secure RFID authentication protocol adopting error correction code