2000-01-01

Thermal Energy Storage-2 (TES-2) is a flight experiment that flew on the Space Shuttle Endeavour (STS-72), in January 1996. TES-2 originally flew with TES-1 as part of the OAST-2 Hitchhiker payload on the Space Shuttle Columbia (STS-62) in early 1994. The two experiments, TES-1 and TES-2 were identical except for the fluoride salts to be characterized. TES-1 provided data on lithium fluoride (LiF), TES-2 provided data on a fluoride eutectic (LiF/CaF2). Each experiment was a complex autonomous payload in a Get-Away-Special payload canister. TES-1 operated flawlessly for 22 hr. Results were reported in a paper entitled, Effect of Microgravity on Materials Undergoing Melting and Freezing-The TES Experiment, by David Namkoong et al. A software failure in TES-2 caused its shutdown after 4 sec of operation. TES-1 and 2 were the first experiments in a four experiment suite designed to provide data for understanding the long duration microgravity behavior of thermal energy storage salts that undergo repeated melting and freezing. Such data have never been obtained before and have direct application for the development of space-based solar dynamic (SD) power systems. These power systems will store energy in a thermal energy salt such as lithium fluoride or a eutectic of lithium fluoride/calcium difluoride. The stored energy is extracted during the shade portion of the orbit. This enables the solar dynamic power system to provide constant electrical power over the entire orbit. Analytical computer codes were developed for predicting performance of a space-based solar dynamic power system. Experimental verification of the analytical predictions were needed prior to using the analytical results for future space power design applications. The four TES flight experiments were to be used to obtain the needed experimental data. This paper will address the flight results from the first and second experiments, TES-1 and 2, in comparison to the predicted results from the Thermal Energy Storage Simulation (TESSIM) analytical computer code. An analysis of the TES-2 data was conducted by Cleveland State University Professor, Mounir Ibrahim. TESSIM validation was based on two types of results; temperature history of various points on the containment vessel and TES material distribution within the vessel upon return from flight. The TESSIM prediction showed close comparison with the flight data. Distribution of the TES material within the vessel was obtained by a tomography imaging process. The frozen TES material was concentrated toward the colder end of the canister. The TESSIM prediction indicated a similar pattern. With agreement between TESSIM and the flight data, a computerized representation was produced to show the movement and behavior of the void during the entire melting and freezing cycles.

479. Secure Multi-party Computation Protocol for Defense Applications in Military Operations Using Virtual Cryptography

NASA Astrophysics Data System (ADS)

Pathak, Rohit; Joshi, Satyadhar

With the advent into the 20th century whole world has been facing the common dilemma of Terrorism. The suicide attacks on US twin towers 11 Sept. 2001, Train bombings in Madrid Spain 11 Mar. 2004, London bombings 7 Jul. 2005 and Mumbai attack 26 Nov. 2008 were some of the most disturbing, destructive and evil acts by terrorists in the last decade which has clearly shown their evil intent that they can go to any extent to accomplish their goals. Many terrorist organizations such as al Quaida, Harakat ul-Mujahidin, Hezbollah, Jaish-e-Mohammed, Lashkar-e-Toiba, etc. are carrying out training camps and terrorist operations which are accompanied with latest technology and high tech arsenal. To counter such terrorism our military is in need of advanced defense technology. One of the major issues of concern is secure communication. It has to be made sure that communication between different military forces is secure so that critical information is not leaked to the adversary. Military forces need secure communication to shield their confidential data from terrorist forces. Leakage of concerned data can prove hazardous, thus preservation and security is of prime importance. There may be a need to perform computations that require data from many military forces, but in some cases the associated forces would not want to reveal their data to other forces. In such situations Secure Multi-party Computations find their application. In this paper, we propose a new highly scalable Secure Multi-party Computation (SMC) protocol and algorithm for Defense applications which can be used to perform computation on encrypted data. Every party encrypts their data in accordance with a particular scheme. This encrypted data is distributed among some created virtual parties. These Virtual parties send their data to the TTP through an Anonymizer layer. TTP performs computation on encrypted data and announces the result. As the data sent was encrypted its actual value canâ€™t be known by TTP and with the use of Anonymizers we have covered the identity of true source of data. Modifier tokens are generated along encryption of data which are distributed among virtual parties, then sent to TTP and finally used in the computation. Thus without revealing the data, right result can be computed and privacy of the parties is maintained. We have also given a probabilistic security analysis of hacking the protocol and shown how zero hacking security can be achieved.

480. Validation of a Natural Language Processing Algorithm for Detecting Infectious Disease Symptoms in Primary Care Electronic Medical Records in Singapore.

PubMed

Hardjojo, Antony; Gunachandran, Arunan; Pang, Long; Abdullah, Mohammed Ridzwan Bin; Wah, Win; Chong, Joash Wen Chen; Goh, Ee Hui; Teo, Sok Huang; Lim, Gilbert; Lee, Mong Li; Hsu, Wynne; Lee, Vernon; Chen, Mark I-Cheng; Wong, Franco; Phang, Jonathan Siung King

2018-06-11