UPM hasilkan Mekanisme Pengkapsulan Kekunci Rabin-p

MENCAPAI TAHAP KESELAMATAN YANG LEBIH TINGGI DAN MUDAH DIGUNAKAN PADA PERISIAN DAN PERKAKASAN

MEKANISME Pengkapsulan Kekunci Rabin-p adalah algoritma penyulitan kekunci awam yang dibina atas masalah pemfaktoran payah integer sebagai sumber keselamatan yang bertujuan untuk penghasilan sistemkripto yang selamat dan cekap.

Dr. Muhammad Asyraf Asbullah dari Institut Penyelidikan Matematik (INSPEM), Universiti Putra Malaysia berkata, kelebihan Mekanisme Pengkapsulan Kekunci Rabin-p termasuk keupayaan untuk membawa data bersaiz lebih besar dengan jaminan tiada kegagalan penyahsulitan.

Menurutnya, ia mencapai tahap keselamatan yang lebih tinggi dan mudah digunakan pada perisian dan perkakasan.

"Rekaan kami hanya menggunakan penyahsulitan nombor perdana tunggal, menyumbang kepada penggunaan memori yang rendah, masa pengiraan yang lebih cepat dan memerlukan ruang penyimpanan yang minimum.

Beliau berkata, insiden kebocoran maklumat adalah pelepasan data sulit atau rahsia kepada persekitaran yang tidak terjamin sama ada secara disengajakan atau tidak berlaku setiap hari.

"Dalam senario Malaysia, sebab utama kebocoran maklumat adalah kerana data tersebut tidak disulitkan sejak dari awal ia dihantar. Oleh itu, pembangunan algoritma penyulitan kekunci awam tempatan dibangunkan sepenuhnya dan siap untuk digunakan diharap dapat mengatasi masalah tersebut," katanya.

MUHAMMAD menerangkan sesuatu kepada pengunjung yang melihat pameran Mekanisme Pengkapsulan Kekunci Rabin-p.

Ciptaan seiring Revolusi Peindustrian 4.0

Dr Muhammad berkata, penyelidikan itu bermula pada 2012 dan berakhir pada 2016 yang telah menerima suntikan dana melalui Skim Latihan Akademi Bumiputera (SLAB) daripada Kementerian Pengajian Tinggi dan Geran Putra – Inisiatif Penyelidik Muda (GP-IPM) daripada Universiti Putra Malaysia.

Beliau bersama kumpulan penyelidik Profesor Madya Dr. Muhammad Rezal Kamel Ariffin dan Zahari Mahad terlibat dalam penghasilan algoritma Mekanisme Pengkapsulan Kekunci Rabin-p. Dr Muhammad Asyraf berkata, ciptaan itu terpakai bagi projek penyelidikan dan pembangunan untuk teknologi perisian, sistem sokongan penyulitan di sebalik teknologi blockchain dan peranti Internet kebendaan, seiring dengan semangat Revolusi Perindustrian 4.0.

"Ciptaan kami ditulis sebagai jujukan pengaturcaraan khusus dalam Bahasa pengaturcaraan C/C ++, Java dan juga PHP yang dapat dibenamkan dengan mudah pada pelbagai platform teknologi termasuk secara atas talian untuk memenuhi keperluan industri hari ini dan keperluan industri masa hadapan.

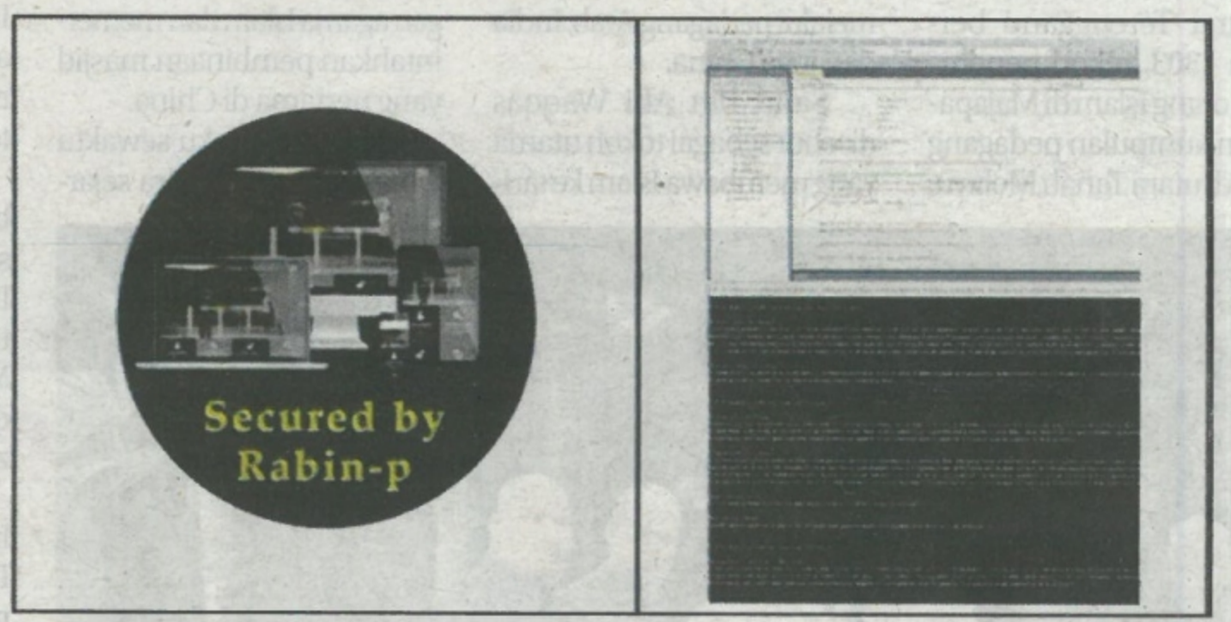
Kelebihan penemuan baharu

"Berbanding dengan produk komersial dan teknologi sedia ada, algoritma ciptaan kami hanya menggunakan nombor perdana tunggal untuk tujuan penyahsulitan, oleh itu mempunyai kelebihan berikut penggunaan memori yang rendah, masa pengiraan lebih cepat dan kurang ruang penyimpanan diperlukan," katanya.

Beliau berkata, ciptaan itu telah berfungsi sepenuhnya dan bersedia untuk dikomersialkan Pada masa ini, ahli pasukan sedang bekerjasama secara aktif dengan sebuah syarikat yang berminat iaitu IEXPLOTECH sebagai rakan kongsi strategik.

"Impak inovasi kami menyokong Dasar Kriptografi Negara melalui pengukuhan komuniti penyelidikan keselamatan siber ke arah kemandirian negara. Selari dengan itu, kami juga mempromosikan pembangunan dan pengkomersilan harta intelek, teknologi, dan inovasi khususnya dalam bidang kriptografi bermatematik melalui penyelidikan dan pembangunan yang terarah, pada masa yang sama memupuk pertumbuhan industri keselamatan siber dalam negara" katanya.

Tambahnya, Mekanisme Pengkapsulan Kekunci Rabin-p telah melalui proses analisis yang ketat oleh pakar kriptografi tempatan di bawah inisiatif Senarai Algoritma Kriptografi Terpercaya Negara (MySEAL) yang diterajui oleh CyberSecurity Malaysia.



MEKANISME Pengkapsulan Kekunci Rabin-p adalah algoritma penyulitan kekunci awam yang dibina atas masalah pemfaktoran payah integer sebagai sumber keselamatan.

"Selaras dengan usaha jangka masa panjang pihak CyberSecurity Malaysia melalui projek Algoritma Kriptografi Baharu (AKBA) MySEAL (untuk tempoh lima tahun: 2016-2020), inovasi kami adalah tercalon dan akan digunakan sebagai keperluan dan panduan mengenai penggunaan algoritma kriptografi dalam semua produk kriptografi terpercaya di Malaysia kelak," katanya.

Sudah sedia dikomersialkan

"Memandangkan algoritma Mekanisme Pengkapsulan Kekunci Rabin-p telah tersenarai pendek untuk algoritma kriptografi kebangsaan di bawah inisiatif AKBA MySEAL dan produk kini bersedia untuk dikomersialkan, maka kami yakin Universiti Putra Malaysia boleh mencapai perjanjian komersil dengan pelbagai organisasi dan manfaat pengeluaran melalui pelbagai mekanisme perkongsian keuntungan," katanya.

Beliau berkata, pihaknya telah mengenal pasti potensi awal pasaran produk tersebut iaitu Agensi Keselamatan Siber Kebangsaan (NACSA), CyberSecurity Malaysia (CSM) dan Prasarana Kunci Awam Kerajaan - GPKI (MAMPU).