Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Erbgut im Angebot

Informatiker der TU Darmstadt entwickeln Schutzmechanismen für Genomdaten

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20018
Fax 06151 16 - 23750
feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 14. Dezember 2016. Je besser Genomdaten erforscht sind, desto gezielter können Ärzte ihre Patienten künftig behandeln. Doch wie lassen sich diese hochsensiblen Daten vor Missbrauch schützen? Informatiker der Technischen Universität Darmstadt möchten sie so geschickt verschlüsseln, dass man dennoch mathematische Analysen mit ihnen durchführen kann.

Genomdaten sind unsere biologische Identität. Aus geerbten genetischen Varianten – den sogenannten SNPs (Single Nucleotide Polymorphisms) – lässt sich zum Beispiel herauslesen, ob wir ein erhöhtes Risiko aufweisen, an Krebs, Huntington Disease oder Parkinson zu erkranken. Für Lebensversicherungen oder Arbeitgeber ist dieses Wissen Gold wert. Forscher fürchten deshalb zu Recht, dass Genomdaten bereits im Internet gehandelt werden – ohne unser Wissen und Einverständnis.

Dennoch ist es keine gute Idee, die Nutzung der Daten generell zu verbieten. Sie sind Grundlage für eine personalisierte Medizin, mit der Ärzte künftig eine auf Patienten zugeschnittene Therapie anbieten können. Die Genomdaten liefern womöglich Hinweise darauf, ob jemand ein Medikament besonders gut vertragen wird oder ob eine bestimmte Therapie anschlagen wird.

Stefan Katzenbeisser und Kay Hamacher vom Profilbereich Cybersecurity (CYSEC) der TU Darmstadt möchten einerseits Genomdaten nutzbar machen und sie andererseits vor Missbrauch schützen. Ein Risiko besteht zum Beispiel immer dann, wenn Ärzte und Kliniken die Daten für die Forschung frei geben. Die Genomforschung ist auf leistungsstarke Rechner angewiesen, daher müssen IT-Dienstleister involviert werden, die mit Super-Computern die Daten durchforsten. „Wir benötigen also ein Verfahren, bei dem die Daten zwar verschlüsselt werden, bei dem aber dennoch nachträgliche Berechnungen möglich sind“, sagt Katzenbeisser. „Der Dienstleister, der die Berechnung durchführt, darf keine Gelegenheit haben, die unverschlüsselten Daten einzusehen.“

Das Verfahren nennt sich homomorphe Verschlüsselung. Ein vereinfachtes Beispiel zeigt, wie es funktioniert: Zwei Zahlen werden als verschlüsselte Werte A und B an einen Dienstleister geschickt. Der Dienstleister multipliziert A und B und schickt das Ergebnis C zurück. Dabei kennt er weder A noch B noch C. Der Auftraggeber hingegen kann C wieder entschlüsseln und das Ergebnis im Klartext auslesen. Auf ähnliche Weise lassen sich auch komplexe Berechnungen durchführen.

Weil Genomdaten zudem aus großen Datensätzen bestehen, konzentrieren sich Forscher bei ihren Analysen meist auf die SNPs oder Mutationen der DNA. Das führt zu einem weiteren Sicherheitsrisiko: Der IT-Dienstleister könnte aus dem Zugriff auf die Sequenz schließen, woran die Forscher arbeiten. „Der DNA-String, den ich untersuche, gibt viel Preis darüber, mit welchen Krankheiten oder Wirkstoffen ich mich beschäftige“, sagt Katzenbeisser. „Um dies zu verhindern, führen wir ein Täuschungsmanöver ein, das sogenannte Oblivious RAM. Dabei wird der physische Speicher bei der Datenbankabfrage ständig durcheinander gemischt. Niemand kann dann nachvollziehen, ob der Fragesteller mehrmals auf die gleichen Daten oder auf unterschiedliche Daten zugegriffen hat. Die Intention der Abfrage ist verschleiert.“
Die Teams von Katzenbeisser und Hamacher möchten zunächst die Basistechniken für die kryptischen Verfahren entwerfen und dann Tools, mit denen sich die Verfahren fehlerfrei umsetzen lassen. Die Forschungen sind Teil des von der Deutschen Forschungsgemeinschaft finanzierten Sonderforschungsbereichs CROSSING und des vom Bundesforschungsministerium geförderten Schwerpunkts CRISP.

Kontakt:
Profilbereich Cybersecurity
Prof. Dr. Stefan Katzenbeisser
E-Mail: katzenbeisser@seceng.informatik.tu-darmstadt.de
Tel.: 06151 16-25620

Prof. Dr. Kay Hamacher
E-Mail: hamacher@bio.tu-darmstadt.de
Tel.: 06151 16-20370

www.cysec.tu-darmstadt.de

MI-Nr. 85/2016, sh /feu