Klaus Pohl. Foto: Vladimir Unkovic

*Persönliche Daten in der Cloud zu speichern und zu verarbeiten, kann ein Risiko sein, wenn die Daten vor Manipulation und unerlaubtem Zugriff nicht sicher sind. Spätestens seit der NSA-Affäre interessiert die Nutzer*innen: Wer besitzt meine Daten? Wer kann darauf zugreifen? Was passiert bei deren Verarbeitung und Auswertung? Wissenschaftler*innen am paluno (The Ruhr Institute for Software Technology) der Universität Duisburg-Essen arbeiten an softwaretechnischen Lösungen zur sicheren Datenverarbeitung beim Cloud Computing.*

Ganz privat?

Der Schutz persönlicher Daten in der Cloud

Von Zoltan Mann, Andreas Metzger & Klaus Pohl

Die Cloud-Dienste im Internet werden immer zahlreicher, komfortabler und sind leicht zu nutzen. Beispiele sind die Apple iCloud, GoogleDocs, Amazon Web Services oder DropBox. Für die Nutzer*innen wird es jedoch zunehmend schwerer nachzuvollziehen, was solche Cloud-Dienste mit den persönlichen Daten machen und ob persönliche Daten in unerwünschte Hände gelangen. Dies liegt daran, dass Clouds und die Anbieter von Cloud-Diensten sich untereinander mehr und mehr vernetzen und somit Daten untereinander austauschen. Um Lastspitzen abzufangen, können Daten und Software-Komponenten auch in andere Cloud-Rechenzentren verschoben werden (sog. Cloud-Migration). Ein Beispiel: Wenn der Andrang auf einer Online-Einkaufsplattform kurz vor Weihnachten sehr hoch ist, erlaubt die Cloud, Daten in andere Rechenzentren auszulagern. Genau diese Flexibilität – im Cloud-Kontext oft auch Elastizität genannt – ist einer der wesentlichen Vorteile der Cloud. Aus Sicht des Datenschutzes birgt sie jedoch zusätzliche Gefahren.

Die Datenschutz-Grundverordnung der EU sieht vor, dass persönliche Daten die EU nicht verlassen dürfen. In dem Beispiel der Online-Einkaufsplattform dürfen die Daten der EU-Bürger*innen nicht außerhalb der Europäischen Union verschoben werden, weil andere Gesetze gelten. Allerdings kann dies dennoch passieren, etwa wenn Cloud-Dienste fehlerhaft entwickelt wurden und somit persönliche Daten zum Beispiel in Cloud-Rechenzentren in den USA verschoben werden.

Cloud-Systeme sind in hohem Maße dynamisch, so dass man zum Schutz persönlicher Daten in der Cloud die sich ständig ändernden Ziele und Rahmenbedingungen berücksichtigen muss. Die Dynamik von Cloud-Systemen hat viele Gründe: Die Rechenlast der Cloud-Dienste ändert sich kontinuierlich je nach Nutzer*innen-Verhalten, Rechner fallen manchmal aus, Software-Komponenten werden zwischen Rechnern migriert und so weiter. Beim Thema Datensicherheit kommen zusätzliche Dimensionen der Dynamik hinzu. Beispielsweise kann ein*e Nutzer*in die Sicherheitseinstufung seiner*ihrer Daten ändern, so dass Datensätze, die bisher nicht geschützt werden mussten, plötzlich als schützenswert eingestuft sind oder umgekehrt. Auch Änderungen von Software-Komponenten können ähnliche Effekte erzeugen, zum Beispiel wenn eine Software-Komponente, die bisher anonymisierte Daten ausgegeben hat, nach einer Programmänderung persönliche Daten ausgibt.

Weitere, subtilere Gefahrenquellen für den Datenschutz gehen von anderen Cloud-Nutzer*innen aus. Um die Kosten niedrig zu halten, ist

es im Cloud Computing üblich, dass Software-Komponenten für unterschiedliche Nutzer*innen auf demselben Rechner im Rechenzentrum laufen, gegebenenfalls gekapselt in sogenannte virtuelle Maschinen, aber immerhin auf derselben physischen Maschine. Dies ermöglicht prinzipiell, dass eine bösartige Software-Komponente eines Nutzers die Daten eines anderen Nutzers, die auf demselben Rechner beheimatet sind, ausspioniert oder verfälscht. Gegen solche Angriffe hilft auch nicht, dass das Rechenzentrum sich in einem erlaubten Land befindet; ein effektiver Schutz kann nur durch geeignete Sicherheitsmechanismen gewährleistet werden.

Lösungsansatz

Um mit dieser oben motivierten vielfältigen Dynamik und den Herausforderungen beim Schutz persönlicher Daten in der Cloud umgehen zu können, ist Adaptionsfähigkeit der Cloud-Systeme gefordert. Ein gutes Fundament dazu bildet das Wissen, das Softwareingenieure in den letzten 10 bis 15 Jahren über so genannte Selbst-adaptierende (Software-)Systeme gesammelt haben. Diese sind Systeme, die in der Lage sind, Änderungen der Umgebung zu beobachten und sich selbst – in vordefiniertem Rahmen – an die Änderungen der Umgebung anzupassen, wie in Abbildung (1) schematisch dargestellt.

Die Grundidee der paluno-Lösungen ist, dieses allgemeine Muster auf das Problem der Datensicherheit in der Cloud anzuwenden. Dazu werden die Konfiguration des Cloud-Systems (inklusive physischer und virtueller Maschinen, Anwendungskomponenten, Datensätze und Datenflüsse) sowie die Datensicherheitsanforderungen der Nutzer*innen kontinuierlich beobachtet. Falls die Beobachtungen potentielle Verletzungen feststellen, passen sich die Cloud-Dienste an, um solche Verletzungen zu verhindern oder zu mitigieren.

Dementsprechend bestehen die paluno-Lösungen aus zwei wesentlichen Pfeilern. Diese sind (1) die Beobachtung der Cloud-Systeme

(1) Adaptive Software-Systeme: Das Bild zeigt die beiden wesentlichen Phasen bei der Selbst-Adaption: Laufzeit-Beobachtung und dynamische Anpassung.
Quelle: paluno

während der Laufzeit und des Betriebs, um mögliche Datenschutzgefährdungen zu erkennen, (2) die dynamische Anpassung der Cloud-Systeme, um auf Datenschutzgefährdungen zu reagieren und diese möglichst zu vermeiden beziehungsweise zu mitigieren.

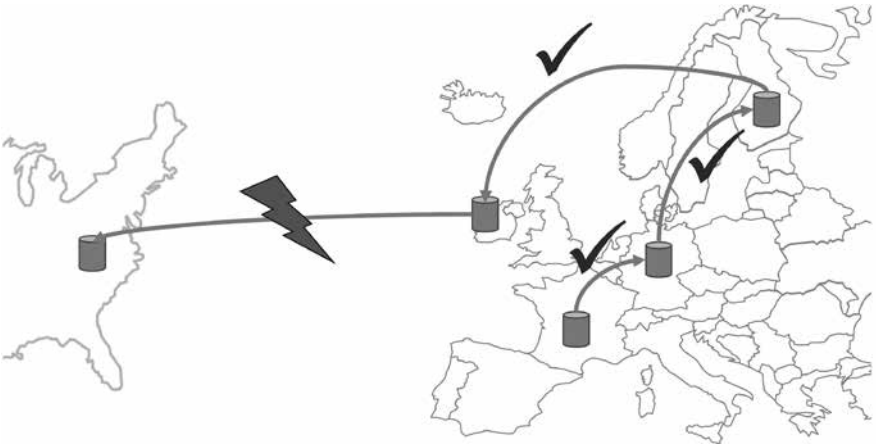
Pfeiler 1: Laufzeit-Beobachtung von Cloud-Systemen

Abbildung (2) zeigt ein plakatives Beispiel, wie es zu einer Verletzung des Datenschutzes beim Betrieb von Cloud-Diensten kommen kann. Persönliche Daten, die in der Cloud gespeichert sind, können in ein entfernt liegendes Datencenter zur Laufzeit verschoben werden. Durch eine solche Verschiebung können somit Daten in eine ausgeschlossene Geo-Lokation gelangen. In dem Beispiel würden etwa unerlaubt persönliche Daten in ein Datencenter in den USA gelangen. Die gezeigten Verschiebungen nach Deutschland, Finnland oder Irland wären in diesem Beispiel jedoch ohne Probleme.

Die Forschungsarbeiten von paluno zur Datenschutz-Beobachtung zielen darauf ab, solche Datenschutzverletzungen während des Betriebs von Cloud-Systemen zu erkennen. Im Rahmen des Gemeinschaftsprojekts iObserve erarbeiten paluno-Wissenschaftler*innen der Arbeitsgruppe von Prof. Klaus Pohl mit Forschungskolleg*innen der Christian-Albrechts-Universität zu Kiel und dem Karlsruher Institut für Technologie neue Techniken zur Cloud-Beobachtung. Das iObserve-Projekt gehört seit 2012 zum Schwerpunktprogramm 1593 „Design For Future – Managed Software Evolution“, das von der Deutschen Forschungsgemeinschaft (DFG) gefördert wird.

Zur Cloud-Beobachtung werden in iObserve neuartige Software-Programme entwickelt, die – sozusagen als Kontrollinstanzen – die Cloud-Systeme automatisiert beobachten, selbst wenn sich ein Cloud-Anbieter nicht beliebig in die Karten schauen lässt. Aus diesen Beobachtungen werden so genannte Laufzeitmodelle abgeleitet. Diese erlauben komplexe Analysen von Daten und Datenflüssen und liefern Hinweise, ob Datenschutzvorgaben eingehalten oder verletzt werden. Ausgehend von diesen Analysen können Handlungsempfehlungen generiert werden, um Datenschutzverletzungen zu verhindern. Insbesondere erlauben die iObserve-Lösungen Verletzungen von Geo-Lokations-Richtlinien zu erkennen. Diese treten auf, wenn Daten in unzulässige Regionen oder Länder verschoben werden (wie im Beispiel in Abb. 2 gezeigt).

Eine solche Cloud-Beobachtung während des Betriebs ist notwendig, da – wie oben erläutert – Software-Komponenten und Daten dynamisch – auch zwischen Rechenzentren – verschoben werden können. Diese Verschiebungen sind zur Entwurfszeit, sprich während der Entwicklung der Cloud-Dienste, nicht bekannt, da sie erst zur Laufzeit zur Optimierung der Performanz, der Verfügbarkeit und der Kosten ausgelöst werden. Durch die dynamische Verschiebung von Software-Kompo-



(2) Verschiebung von Daten zwischen Cloud-Rechenzentren kann zu Datenschutzverletzungen führen. Verschiebung innerhalb der EU ist laut EU-Datenschutz-Grundverordnung zulässig, jedoch nicht eine Verschiebung von Daten von EU-Bürger*innen in die USA.
Quelle: paluno

nenten, wie zum Beispiel von Datenbanken oder Komponenten zur Datenanalyse, könnten Daten in unerlaubte Länder gelangen.

Der in iObserve entwickelte Ansatz zur Datenschutz-Beobachtung von Cloud-Systemen würde eine Verletzung wie die in Abbildung (2) erkennen. In solchen Fällen erkennt der iObserve-Ansatz, dass eine potentielle Verletzung der Datenschutzrichtlinien aufgetreten ist, und kann somit die dynamische Anpassung der Cloud-Systeme auslösen.

Pfeiler 2: Dynamische Anpassung von Cloud-Systemen

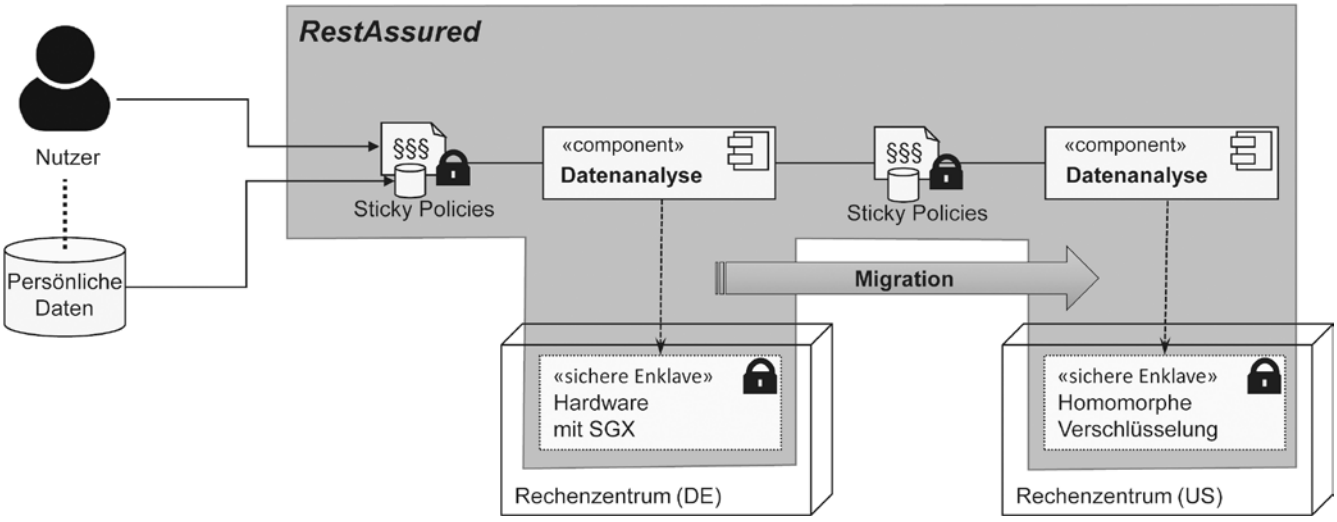
In den letzten Jahren gab es in den Bereichen der Systemsicherheit und der Kryptographie große Fortschritte und es wurden Sicherheitsmechanismen erarbeitet, die prinzipiell das Potenzial haben, die speziellen Sicherheitsbedenken in der Cloud zu adressieren. Diese Sicherheitsmechanismen bieten zusätzliche Anpassungsmöglichkeiten, die bei der dynamischen Anpassung von Cloud-Systemen genutzt werden können.

Das von der Europäischen Union geförderte Projekt „RestAssured – Secure Data Processing in the Cloud“ hat zum Ziel, mit Hilfe neuartiger Sicherheitsmechanismen Datensicherheit in der Cloud zu gewährleisten. In RestAssured arbeiten paluno-Wissenschaftler*innen der Arbeitsgruppen von Prof. Maritta Heisel und Prof. Klaus Pohl mit namhaften Partnern aus Forschung und Industrie zusammen, unter anderem mit IBM, Thales und der Universität Southampton. Gemeinsam werden Lösungen erarbeitet, die auf den neuesten wissenschaftlichen Erkenntnissen aufsetzen und gleichzeitig für den praktischen Einsatz tauglich sind.

Als konkrete Maßnahmen zur Anpassung des Systems mit dem Ziel des Datenschutzes werden in RestAssured drei innovative Sicherheitstechniken eingesetzt.

Hardware-Enklaven sind virtuelle Bereiche eines Hardware-Speichers, in denen Software-Komponenten ihre Daten und ihren Code sicher speichern können. Dadurch ist es möglich, sowohl die Daten als den Code kritischer Cloud-Dienste vor unbefugtem Zugriff zu schützen. Der Schutz ist wirksam nicht nur gegen Angriffe anderer Nutzer*innen, sondern sogar gegen potenzielle Angriffe seitens des Rechenzentrumbetreibers. Das Konzept von Hardware-Enklaven ist schon seit einigen Jahren bekannt. 2016 hat der Chiphersteller Intel mit dem SGX-Befehlssatz (Software Guard Extensions) erste Prozessoren auf den Markt gebracht, die dieses Konzept tatsächlich auch umsetzen. Diese Chips nehmen langsam Einzug in die Cloud-Rechenzentren. Allerdings kann man nicht davon ausgehen, dass auch in absehbarer Zeit alle Rechner diese Sicherheitsmechanismen unterstützen werden. Aus diesem Grund kann man SGX auch nicht per se einsetzen, sondern nur für die konkreten Fälle, in denen die Vermeidung von Datenschutzverletzungen angezeigt ist, und insoweit diese Mechanismen im konkreten Cloud-Rechenzentrum verfügbar sind.

Vollhomomorphe Verschlüsselung ist eine revolutionäre kryptographische Methode, die ein direktes Arbeiten auf dem Chiffretext ermöglicht. Traditionell werden verschlüsselte Daten zuerst entschlüsselt um anschließend verarbeitet werden zu können. Dies hat zur Folge, dass der Cloud-Dienst, der die Verarbeitung durchführt, zwangsläufig Zugriff auf die Daten bekommt und somit eine Sicherheitslücke darstellt. Im Gegensatz dazu brauchen die Daten bei homomorpher Verschlüsselung nicht entschlüsselt zu werden: Die nötigen Verarbeitungsschritte können direkt an den verschlüsselten Daten durchgeführt werden. Das bedeutet, dass die verarbeitende Anwendung die eigentlichen Daten gar nicht kennen muss, was die Risiken bezüglich Datensicherheit deutlich reduziert. Dass ein Verschlüsselungsverfahren mit den nötigen, sogenannten Homomorphie-Eigenschaften überhaupt existiert, wurde erst vor wenigen Jahren von Forscher*innen bei IBM nachgewiesen. Die heute bekannten homomorphen Verschlüsselungsverfahren sind entweder im Umfang der unterstützten Operationen eingeschränkt oder sind zu langsam für die praktische Anwendung, aber die großen Fortschritte der letzten Jahre lassen hoffen, dass vollhomomorphe Verschlüsselung in



(3) Beispiel für die Verwendung innovativer Sicherheitstechniken im Projekt RestAssured. Nutzer*in legen Datensicherheitsanforderungen mittels Sticky Policies fest. Bei einer Verschiebung der Daten aus Deutschland in die USA wird automatisch homomorphe Verschlüsselung eingesetzt, so dass keiner außer dem*der Nutzer*in Zugriff auf die Daten in unverschlüsselter Form erlangt.
Quelle: paluno

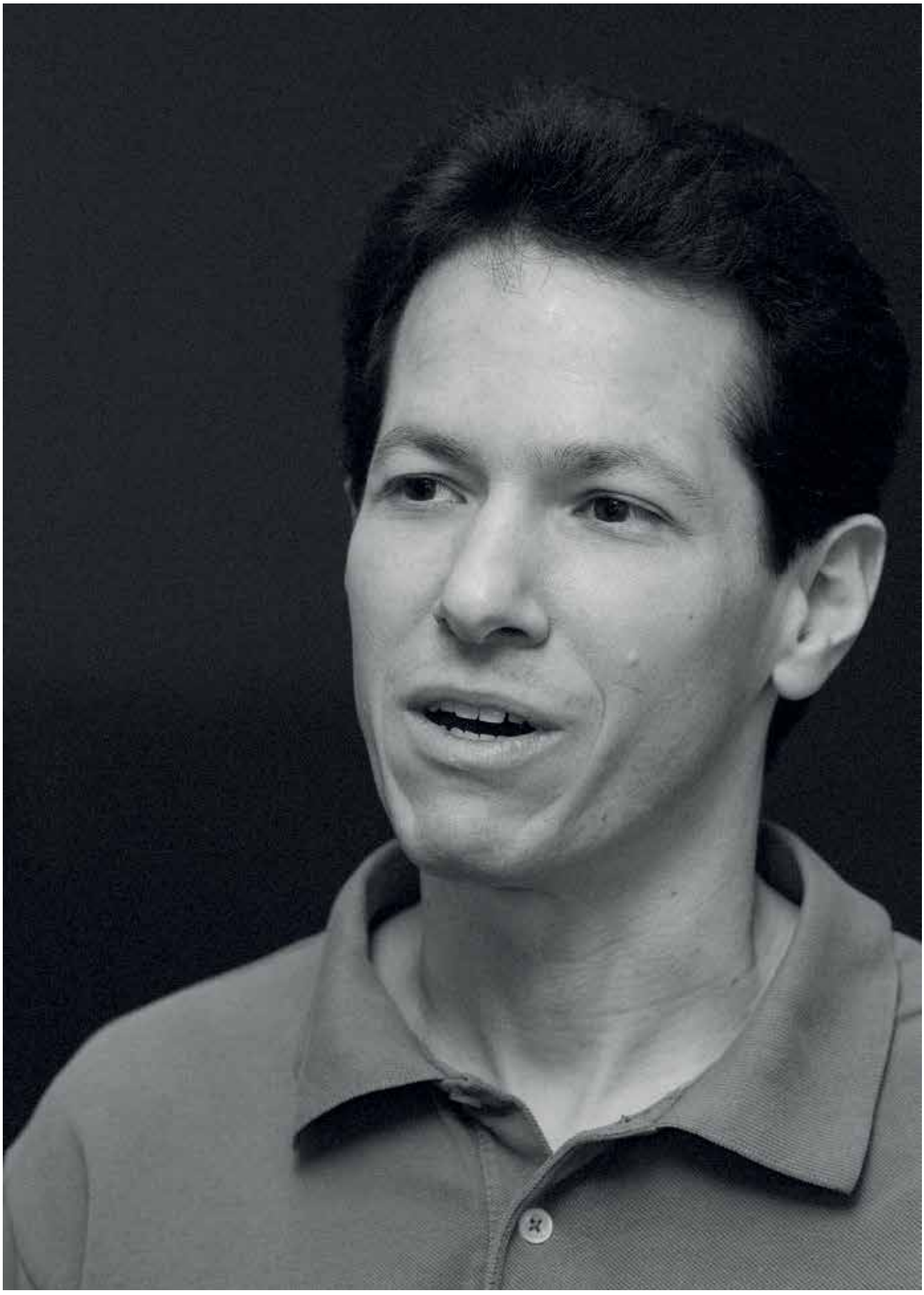
absehbarer Zukunft zu einer marktreifen Technologie wird. Wegen der Performanzeinbußen sollte vollhomomorphe Verschlüsselung auf jeden Fall nur dann eingesetzt werden, wenn die Vermeidung von Datenschutzverletzungen angezeigt ist.

Sticky Policies ermöglichen die Kennzeichnung der Kritikalität einzelner Datensätze. Dadurch kann gesteuert werden, wer welche Operationen auf diesen Datensätzen durchführen darf. Durch entsprechende kryptographische Verfahren wird sichergestellt, dass bei einer Bewegung des Datensatzes (z.B. Migration) auch die zugehörige Sticky Policy mitgeht (daher die Benennung „sticky“, da sie an dem Datensatz haftet) und auch eingehalten wird. Im Projekt RestAssured sorgt ein verteiltes Management der Sticky Policies dafür, dass der gesamte Lebenszyklus der Daten kontrolliert wird und der Schutzbedarf der Daten stets korrekt bestimmt ist.

Diese Sicherheitsmechanismen, zusammen mit den üblichen Anpassungsmechanismen von Cloud-Systemen (wie z.B. die Migration von virtuellen Maschinen zwischen physischen Maschinen) stellen die Grundlagen für eine integrierte und adaptive Datensicherheitslösung dar. Insbesondere können Sticky Policies genutzt werden, um die Datensicherheitsanforderungen zu spezifizieren und später auch zu ändern. Solche Änderungen können beobachtet werden und somit als Auslöser für Anpassungen dienen. Mögliche Anpassungen umfassen die Migration zwischen physischen Maschinen mit und ohne Hardware-Enklaven oder das Ein- und Ausschalten von homomorpher Verschlüsselung, wie auch in Abbildung (3) schematisch dargestellt.

Wichtig bei der Wahl einer geeigneten Anpassung ist, dass eine konkrete Anpassungsmöglichkeit neben einer Auswirkung auf die Sicherheitseigenschaften auch Nebenwirkungen auf andere Qualitätsattribute wie Performanz oder Kosten umfasst. Beispielsweise hat, wie oben erwähnt, die vollhomomorphe Verschlüsselung einen sehr hohen Rechenbedarf und damit eine Auswirkung auf Qualitätsattribute wie „Durchsatz“ oder „Antwortzeit“. Aufgrund der unterschiedlichen Auswirkungen der jeweiligen Anpassungsmöglichkeiten auf Datensicherheit und andere Qualitätsattribute ergeben sich daher verschiedene mögliche Anpassungsalternativen, aus welchen sich verschiedene Optima auswählen lassen basierend auf der relativen Wichtigkeit der einzelnen Optimierungskriterien.

Die im Projekt RestAssured erarbeiteten Lösungen werden anhand praktischer Anwendungsfälle validiert. Ein Anwendungsfall bezieht sich auf eine Online-Plattform für Pflegedienste, auf der die Zuordnung zwischen Pfleger*innen und Pflegebedürftigen verwaltet wird. Dabei kommt dem Schutz der Daten der Pflegebedürftigen eine besondere Bedeutung zu, da insbesondere auch medizinische Daten der Pflegebedürftigen gespeichert sind. Bei einem weiteren Anwendungsfall handelt es sich um eine fahrverhaltensbasierte Kfz-Versicherung, in der Sensoren im Automobil Daten über das Fahrverhalten der Autofahrer*innen erfassen und an ein Cloud-System senden. In der Cloud werden die gesammelten Daten ausgewertet und daraus die Versicherungsgebühren berechnet. Auch hier spielt der Schutz persönlicher Daten eine große Rolle.



Zoltan Mann. Foto: Vladimir Unkovic

Andreas Metzger. Foto: Vladimir Unkovic

Zusammenfassung

Die sichere Speicherung und Verarbeitung persönlicher Daten in der Cloud ist eine große Herausforderung. Solange dieses Problem nicht gelöst ist, kann man von den Vorteilen des Cloud Computing in Bereichen mit kritischen Daten nur sehr beschränkt profitieren.

Die kontinuierliche Datenschutz-Beobachtung stellt eine wichtige Grundlage für zukünftige Sicherheitslösungen dar. Insbesondere die Verletzung von gesetzlich vorgegebenen Geo-Lokations-Richtlinien wird im Projekt iObserve von Wissenschaftler*innen der UDE behandelt. Im Projekt RestAssured geht man einen Schritt weiter und nutzt innovative Sicherheitsmechanismen um die Cloud-Dienste bei einer möglichen Datenschutzverletzung anzupassen. Durch eine solche Anpassung an veränderte Rahmenbedingungen, beziehungsweise Sicherheitsanforderungen, zielt man darauf ab, Sicherheitsanforderungen stets in optimaler Weise zu erfüllen.

Summary

Cloud computing has many benefits for service providers and service users alike. However, by storing and processing data in the cloud, users lose control over their data. The data security breaches that became publicly known in the last couple of years have shown that this is a real threat that can hinder the adoption of cloud computing, especially in domains with strong data security requirements.

Researchers at paluno (The Ruhr Institute for Software Technology) are working to address this challenge as part of two ongoing research projects. The developed solutions consist of two main pillars: (1) monitoring the adherence to data protection requirements, which is developed in the iObserve project, and (2) adapting the cloud system to react to – actual or imminent – requirements violations, which is developed in the RestAssured project.

In the iObserve project, funded by the DFG, the focus is on monitoring data security in a cloud system. Through appropriate mechanisms, the violation of security requirements can be detected at runtime, making it possible to avoid or mitigate security breaches. In particular, violations of geo-location policies can be detected and appropriate counter-measures may be taken.

In the RestAssured project, funded by the European Union, the focus is on adaptation by leveraging innovative security mechanisms such as hardware enclaves and homomorphic encryption to guarantee security in an adaptive and integrated way. By also considering the impact of the used security mechanisms on other quality attributes like costs and performance, security requirements can be fulfilled in a globally optimal way.

Danksagung

Die vorgestellten Forschungsarbeiten werden gefördert im Rahmen des Schwerpunktprogramms SPP1593: „Design For Future – Managed Software Evolution“ der Deutschen Forschungsgemeinschaft (DFG) unter Förderkennzeichen PO 607/3 (iObserve), sowie im Rahmen des EU Horizon 2020 Forschungs- und Innovationsprogramms unter Förderkennzeichen 731678 (RestAssured).

Literatur

– E. Schmieders, A. Metzger, K. Pohl (2017): Modellbasierte Datenschutzprüfung datenintensiver Cloud Dienste, In: Jan Jürjens, Kurt Schneider (Hrsg.): Software Engineering 2017, Hannover, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn.
– Z. Mann, A. Metzger (2017): Optimized Cloud Deployment of Multi-tenant Software Considering Data Protection Concerns. In: J. Carretero, M. Parashar, J. Garcia-Blas, G.C. Fox, F. Cappello (Hrsg.): 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2017), Madrid, IEEE.
– E. Schmieders, A. Metzger, K. Pohl (2015): Runtime Model-Based Privacy Checks of Big Data Cloud Services. In: A. Barros, D. Grigori, N.C. Narendra, H.K. Dam (Hrsg.): Service-Oriented Computing: Proceedings of the 13th International Conference on Service Oriented Computing (ICSOC 2015), Paris, LNCS 9435, Springer, Berlin, Heidelberg.
– E. Schmieders, A. Metzger, K. Pohl (2014): A Runtime Model Approach for Data Geo-Location Checks of Cloud Services. In: X. Franch, A.K. Ghose, G.A. Lewis, S.Bhiri (Hrsg.): Service-Oriented Computing: Proceedings of the 12th International Conference on Service Oriented Computing (ICSOC 2014), Ghoa, LNCS 8831, Springer, Berlin, Heidelberg.

Die Autoren

Zoltan Mann ist wissenschaftlicher Mitarbeiter am paluno (The Ruhr Institute for Software Technology) an der Universität Duisburg-Essen. Er studierte Informatik und Mathematik in Budapest (Ungarn), wo er 2005 in Informatik promovierte. Zwischen 2004 und 2014 arbeitete er bei verschiedenen Unternehmen in den Bereichen Softwareentwicklung, IT-Beratung und Unternehmensberatung in Deutschland und Ungarn. Zwischen 2007 und 2016 war er an der Technischen und Wirtschaftswissenschaftlichen Universität Budapest beschäftigt, anfangs als „Assistant Professor“, später als „Associate Professor“.

Andreas Metzger ist Akademischer Oberrat an der Universität Duisburg-Essen und Leiter der Bereiche Adaptive Systeme und Big Data Anwendungen am paluno (The Ruhr Institute for Software Technology). Er ist stellvertretender Generalsekretär der Europäischen Big Data Value Association (BDVA) und Vize-Vorstand der Europäischen Technologieplattform NESSI (Networked European Software and Services Initiative). Er studierte Informatik an der TU Kaiserslautern, wo er 2004 in Informatik zum Dr.-Ing. promovierte.

Klaus Pohl ist Professor für Software Systems Engineering an der Universität Duisburg-Essen und Direktor von paluno (The Ruhr Institute for Software Technology). Von 2005 bis 2007 war er wissenschaftlicher Gründungsdirektor des Irish Software Engineering Research Centre (lero). Er ist Vorstandsmitglied der Europäischen Technologieplattform NESSI (Networked European Software and Services Initiative) und Mitglied des Lenkungsausschusses der deutschen Innovations-Allianz SPES (Software-Plattform for Embedded Systems).

Drei Forscher der Universität Duisburg-Essen haben sich nach mehreren Jahren Forschung mit der Firma Locoslab selbständig gemacht. Locoslab GmbH ist ein 2012 ins Leben gerufene Spin-off der Universität, das cloud-basierte Produkte und Dienstleistungen rund um das Thema Lokalisierung anbietet. Vielfältige Anwendungsmöglichkeiten durch den technischen Einsatz des so genannten RF (Radio Frequencing) Fingerprinting, beispielsweise in den Bereichen Navigation auf Flughäfen, in Einkaufszentren oder auf Messen. So können personalisierte Mobilitätslösungen realisiert werden.

SIMON macht mobil

Die Cloud ermöglicht personalisierte Mobilität

Von Pedro José Marrón

Als Teil der Aktivitäten im Bereich personalisierte Mobilität, haben sich Mitarbeiter*innen der Firma Locoslab gemeinsam mit Forscher*innen der Universität Duisburg-Essen der Herausforderung gestellt, Navigationsanwendungen zu implementieren, die für Personen mit eingeschränkter Mobilität besonders relevant sind. Im Rahmen des SIMON EU-Projekts wurden unter anderem Lösungen für multimodales Routing erforscht, die in der Lage sind, Outdoor- und Indoor-Routing nahtlos zu kombinieren. Die Integration dieser Lösungen ist in einer App namens SIMON Mobile erfolgt, die für Android und iOS verfügbar ist.

Erfahrungen mit Indoor Navigation in SIMON Mobile

Mit der Ausbreitung GPS-fähiger Geräte haben sich mobile Navigationsanwendungen zu einem weit verbreiteten Werkzeug entwickelt, die Menschen während ihrer täglichen Fahrten unterstützen. Da GPS in Gebäuden nicht verfügbar ist, werden solche Anwendungen meist nur im Außenbereich genutzt. Infolgedessen kann eine nahtlose End-to-End Nutzung nicht gewährleistet werden. Dies ist besonders dann problematisch, wenn man schnell durch ein Gebäude laufen muss, um zum Beispiel eine bestimmte U-Bahn Haltestelle zu erreichen.

Das Ziel des Europäischen Forschungsprojektes SIMON ist die Entwicklung von Tools und technischen Lösungen, die eine Verbesserung der Mobilität von Menschen mit Einschränkungen ermöglichen. Eine dieser Lösungen ist eine mobile Navigationsanwendung, die speziell für Nutzer*innen mit Geh- oder Sehbehinderungen konzipiert wurde. Die Anwendung wird zur Zeit in Lissabon, Parma, Reading und Madrid getestet.

Ein wichtiger Teil der Anwendung ist die Bereitstellung von nahtlosen und multimodalen Navigationsrouten, die sowohl im Außen- wie im Innenbereich funktionieren und verschiedene Verkehrsmittel wie