Situativer Datenschutz im Fog-Computing[1]

Zoltán Ádám Mann, Andreas Metzger, Klaus Pohl
paluno – The Ruhr Institute for Software Technology, Universität Duisburg-Essen
{zoltan.mann, andreas.metzger, klaus.pohl}@paluno.uni-due.de

Zusammenfassung

Fog-Computing erlaubt Software-Code oder Daten dynamisch von ressourcenschwachen Endgeräten an leistungsstärkere Geräte am Rande des Netzwerks und in der Cloud auszulagern. Eine solche dynamische Auslagerung ermöglicht eine performante Ausführung rechenintensiver Aufgaben, bei gleichzeitig geringer Latenzzeit für die Datenübertragung. Beim Datenschutz ergeben sich im Fog-Computing jedoch spezifische Herausforderungen. Wir beschreiben die wesentlichen Herausforderungen des Datenschutzes im Fog-Computing und diskutieren wie diese Herausforderungen durch die situative Kombination verschiedener Datenschutztechniken zur Laufzeit adressiert werden können.

Abstract

Fog computing makes it possible to dynamically offload software code or data from resource-constrained end devices to computing units with higher capacity near the edge of the network and in the cloud. This facilitates executing resource-intensive tasks with high performance, while keeping the latency for data transfer low. However, data protection in fog computing leads to specific challenges. We describe important challenges for data protection in fog computing, and discuss how these challenges may be addressed by a situational combination of different data protection techniques at run time.

Einleitung

Das Schlagwort „Fog-Computing“ beschreibt den nächsten Schritt in der Virtualisierung von Rechnerressourcen (wie CPU und Speicher) [29]. Ging es beim Cloud-Computing noch um die Virtualisierung der Ressourcen von Rechenzentren [24], erweitert Fog-Computing diese Virtualisierung auf Ressourcen von Endgeräten und sogenannten Edge-Ressourcen. Endgeräte umfassen Smartphones sowie intelligente Sensoren und Aktuatoren aus dem Internet der Dinge [14]. Edge-Ressourcen umfassen Internet-Router und Mobilfunk-Basisstationen. Diese erweiterte Virtualisierung erlaubt es Software-Code auf allen diesen Geräten auszuführen sowie Software-Code und Daten dynamisch auf diese Geräte zu verteilen.

Die dynamische Verteilung von Software-Code und Daten auf diese Geräte bringt deutliche Vorteile und erschließt somit gänzlich neue Anwendungsmöglichkeiten. Im Vergleich zu einer Auslagerung in die Cloud (also in ein entferntes Rechenzentrum) führt der Fog-Computing-Ansatz durch die Nutzung von Edge-Ressourcen zu deutlich geringeren Latenzzeiten bei der Datenübertragung: Edge-Ressourcen befinden sich näher bei den Endgeräten und daher werden deutlich weniger Netzwerk-Hops benötigt. Dies ist insbesondere für zeitkritische Anwendungen essenziell [22]. Beispielsweise sind bestimmte Aufgaben bei der Analyse großer Datenmengen („Big Data“ [28]) mit Fog-Computing in unmittelbarer Nähe der Sensoren, also der Datenquellen, möglich.

[1] Veröffentlicht im *Informatik Spektrum*, 42(4):236-243, 2019. DOI: 10.1007/s00287-019-01190-1

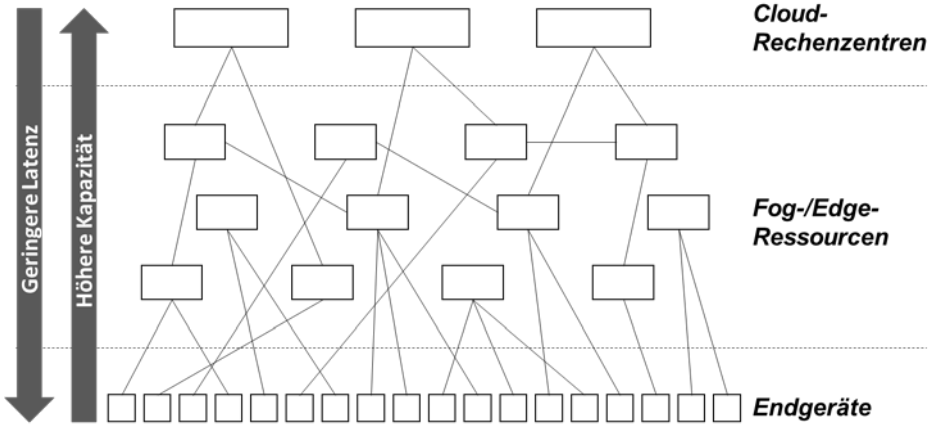

Abb. 1: Fog-Computing ermöglicht die Kombination von Endgeräten, verteilten Edge-Ressourcen am Rand des Netzwerks, sowie Cloud-Ressourcen

Im Fog-Computing ergibt sich grob eine Hierarchie aus drei Ebenen (siehe auch Abb. 1), über welche Software-Code und Daten verteilt werden können:

- *Endgeräte*, die durch stark eingeschränkte Ressourcen gekennzeichnet sind, aber potenziell in sehr hoher Anzahl verfügbar sind;
- *Edge-Ressourcen*, die am Rand des Netzwerks bereitgestellt werden, und damit mit geringer Latenz rechenintensive Aufgaben von den Endgeräten übernehmen können;
- *Cloud-Rechenzentren*, die über eine hohe Kapazität an Ressourcen verfügen.

Wie oft bei neuen Technologien, existiert keine einheitliche Terminologie. Beispielsweise wird der Begriff Edge-Computing auch synonym zu Fog-Computing verwendet, andere Autoren betrachten Edge-Computing als einen Teil des Fog-Computings. In diesem Beitrag nutzen wir den Begriff Fog-Computing für das übergreifende Paradigma, in dem – wie oben beschrieben – die Ressourcen von Endgeräten, der Edge und der Cloud kombiniert verfügbar sind. Den Begriff Edge verwenden wir spezifisch für den Rand des Netzwerks, insbesondere um die dort bereitgestellten Edge-Ressourcen zu beschreiben.

Ein wichtiger Aspekt des Fog-Computings ist die Mobilität der Endgeräte, wie z. B. im Fall von Smartphones. Selbst Edge-Ressourcen sind nicht unbedingt ortsgebunden. Als Beispiel kann hier ein zukünftiges Automobil dienen. Verschiedene Sensoren sammeln während der Fahrt kontinuierlich Daten über Fahrverhalten, Verbrauch etc. Diese Daten können an ein zentrales Steuergerät des Fahrzeugs übermittelt werden, welches in diesem Fall als Edge-Ressource aus Sicht der Sensoren fungiert. Im Steuergerät wird auf Basis der gesammelten Daten die Art des Fahrstils bestimmt und über eine Mobilfunkverbindung an eine Anwendung in der Cloud geschickt. Die Cloud-Anwendung, die z. B. von einer Versicherung genutzt wird, kann den Fahrstil bei der Berechnung der Versicherungsgebühren der Fahrer berücksichtigen. Dadurch können z. B. vorsichtige Fahrer durch niedrigere Versicherungsgebühren belohnt werden. Durch die Vorverarbeitung in der Edge-Ressource im Automobil müssen deutlich geringere Datenumfänge an die Cloud übermittelt werden.

Fog-Computing vereint also verschiedene Ressourcen so, dass die Möglichkeiten und Vorteile der einzelnen Ressourcen geeignet kombiniert und wichtige Systemparameter wie Latenzzeit, Datenübertragung oder Energiebedarf optimiert werden können. Wie jede neue Technologie, so bringt auch das Fog-Computing neue Probleme mit sich. Ein wichtiges Problem ist der Schutz sensibler Daten in Fog-Systemen [30]. Wie im obigen Beispiel angedeutet, können Fog-Systeme sensible Daten verarbeiten; im Beispiel personenbezogene Daten über den Fahrer. Fog-Computing bietet böswilligen Akteuren zahlreiche Möglichkeiten, sich Zugang zu sensiblen Informationen zu verschaffen oder sensible Informationen zu manipulieren [23].

Dieser Artikel beleuchtet die spezifischen Herausforderungen für den Datenschutz im Fog-Computing. Auch wenn zahlreiche Sicherheitstechniken bekannt sind, mit denen der Zugriff auf sensible Daten geschützt werden kann, lassen sich diese Sicherheitstechniken nicht pauschal einsetzen, um die Datenschutzherausforderungen im Fog-Computing zu adressieren. Existierende Sicherheitstechniken haben gewisse Nachteile (z. B. einen zu hohen Ressourcenaufwand für die Edge [1]) oder technische Einschränkungen (z. B. die Notwendigkeit von Spezial-Hardware [11]). Zudem können sich die Konfiguration und die Eigenschaften eines Fog-Systems zur Laufzeit ständig ändern. Es ist daher notwendig, existierende Sicherheitstechniken *situativ* einzusetzen. Das heißt, dass abhängig von der jeweils aktuellen Situation geeignete Sicherheitstechniken selektiert und zur Laufzeit genutzt werden.

Herausforderungen für den Datenschutz im Fog-Computing

Fog-Computing erbt zahlreiche Datenschutz-Herausforderungen vom Cloud-Computing. Die einschlägige Fachliteratur [1][6][17][23][30] ist sich jedoch einig, dass Fog-Computing Eigenschaften besitzt, die zu spezifischen Herausforderungen für den Datenschutz führen. Im Folgenden erläutern wir diese Herausforderungen, gruppiert in (1) Herausforderungen aufgrund der hohen Dynamik von Fog-Systemen und (2) Herausforderungen aufgrund der Charakteristika der Fog-Geräte.

(1) Datenschutz-Herausforderungen aufgrund der hohen Dynamik von Fog-Systemen:

- **Dynamische Veränderung der Datenschutzrisiken durch Dynamik an der Edge**. Im Vergleich zu einem Cloud-System, das bereits eine gewisse Dynamik aufweist (z. B. kann die Last der einzelnen Cloud-Dienste mit der Zeit variieren), entsteht in einem Fog-System mit mobilen Endgeräten eine deutlich höhere Dynamik. Zum Beispiel können sich Endgeräte dynamisch an Edge-Ressourcen binden und von diesen trennen [2][15]. Dies führt u. a. auch zu einer Veränderung der Datenschutzrisiken. Zum Beispiel ist das Risiko aus Sicht eines Endgerätes niedriger, wenn es sich an eine bekannte und zuverlässige Edge-Ressource anbindet. Bricht diese Verbindung ab und ist daher eine Verbindung mit einer bisher unbekannten Edge-Ressource herzustellen, so bedeutet dies für das Endgerät ein höheres Risiko.
- **Dynamische Änderung der Datenschutzanforderungen durch Mobilität**. Durch die Mobilität der Endgeräte und ggf. der Edge-Ressourcen kann es vorkommen, dass ein Fog-Gerät in ein anderes Land mit anderer Rechtsprechung gerät, wodurch sich die Datenschutzanforderungen ändern. Das passiert z. B., wenn das eingangs erwähnte Automobil, das personenbezogene Daten über seinen Fahrer sammelt und speichert, über die EU-Außengrenze fährt. Die EU-Datenschutzgrundverordnung definiert spezielle Auflagen für die Speicherung personenbezogener Daten in Drittstaaten.
- **Unbefugter Datenzugriff aufgrund Unklarheit über relevante Stakeholder**. Im Cloud-Computing wählt ein Nutzer typischerweise explizit und bewusst einen Cloud-Anbieter aus, und muss dabei auch explizit der Nutzung seiner Daten zustimmen. Im Fog-Computing ist hingegen vorgesehen, dass ein Endgerät selbstständig zur Laufzeit verschiedene Fog-Ressourcen in Anspruch nimmt um Aufgaben an diese Fog-Ressourcen auszulagern. Der Nutzer weiß nicht unbedingt, wer diese Fog-Ressourcen bereitstellt und wer potenziell Zugriff auf diese Ressourcen hat. Betreiber oder andere Nutzer der Edge-Ressourcen könnten unberechtigt Zugriff auf sensible Daten erlangen, ohne dass der Nutzer über dieses Risiko Kenntnis hat.

(2) Datenschutz-Herausforderungen bedingt durch die Charakteristika von Fog-Geräten:

- **Beschränkte Ressourcen der Fog-Geräte**. Existierende Techniken für den Datenschutz, wie z. B. kryptografische Algorithmen, sind typischerweise ressourcenintensiv. Für Endgeräte mit stark begrenzter Berechnungs-, Speicher- und Batteriekapazität ist das ein Problem. Dadurch wird der Lösungsraum für mögliche Datenschutzmechanismen im Fog-Computing eingeschränkt.
- **Heterogenität der Fog-Geräte**. Sowohl bei Endgeräten als auch bei Edge-Ressourcen ist die Variantenvielfalt praktisch unbegrenzt. Die Umsetzung einheitlicher Sicherheitsstandards in Fog-Systemen über alle Geräte hinweg ist daher schwierig. Man muss vielmehr damit umgehen können, dass die verschiedenen Geräte unterschiedliche Datenschutzmechanismen unterstützen und zudem unterschiedliche Verwundbarkeiten aufweisen.
- **Schwierigkeiten beim physischen Schutz von Fog-Ressourcen**. Während Cloud-Rechenzentren typischerweise durch strenge physische Zutrittskontrollmechanismen (z. B. Kontrolle der Mitarbeiterausweise und Protokollierung der Ein- und Austritte) geschützt werden [3], können Fog-Computing-Systeme praktisch überall, unter sehr unterschiedlichen Bedingungen eingesetzt werden. Potentielle Angreifer können daher leichter einen physischen Zugriff auf das System erlangen.
- **Direkter Zugriff auf vertrauliche Informationen in der Fog**. Bei der Nutzung von Edge-Ressourcen kann ein Endgerät persönliche Daten der Nutzer offenlegen, und dies sogar ohne eine explizite Datenübertragung an die verwendeten Edge-Ressourcen. Ein Beispiel: Da ein Endgerät Edge-Ressourcen nutzt, die sich in der Nähe des Endgerätes befinden, könnte ein Angreifer auf Basis der Informationen, wann das Endgerät welche Edge-Ressourcen genutzt hat, den Ort bzw. die Route eines Nutzers herausfinden und damit die Privatsphäre des Nutzers beeinträchtigen [6][17].

Im Folgenden zeigen wir auf, dass die Adressierung der Herausforderungen für den Datenschutz im Fog-Computing eine situative Kombination verschiedener Datenschutztechniken erfordert.

Situativer Datenschutz

Es gibt zwei wesentliche Gründe, warum Datenschutzmechanismen im Fog-Computing situativ kombiniert werden sollten. Einerseits ist das durch die oben beschriebene hohe Dynamik von Fog-Systemen begründet [18]. Auf die ständigen Änderungen der Datenschutzanforderungen und -risiken muss zur Laufzeit situativ reagiert werden. Andererseits ist dies durch die Charakteristika der Fog-Geräte begründet. Die Heterogenität und die Ressourcenbeschränkung der Geräte erlauben nicht pauschal eine für alle Situationen geeignete Sicherheitstechnik einzusetzen. Vielmehr ist eine situative Auswahl der Sicherheitstechnik nötig. Abb. 2 detailliert die Einflussfaktoren für die Anwendung existierender Datenschutztechniken auf Basis der jeweiligen Situation.

Abb. 2: Situative Kombination von Datenschutztechniken, um mit der Dynamik von Fog-Systemen und den Charakteristika der Fog-Geräte umzugehen

Die linke Seite von Abb. 2 zeigt, dass auf die dynamischen Änderungen bei Datenschutzanforderungen und -risiken situativ reagiert werden muss. Unter dem Schlagwort „Security by design“ bzw. „Privacy by design“ wird versucht, Systeme so zu entwerfen, dass sie die Erfüllung gewisser Datenschutzziele garantieren. Aufgrund der hohen Dynamik von Fog-Systemen genügen diese Ansätze allerdings nicht mehr. Zur Entwicklungszeit der Systeme ist zum Beispiel nicht bekannt, welche konkreten Edge-Ressourcen zur Laufzeit existieren werden. Daher ist die konkrete Verteilung von Software-Code auf die Fog-Ressourcen zur Entwicklungszeit nicht bekannt und steht erst zur Laufzeit fest. Auch sind die zur Laufzeit geltenden Datenschutzanforderungen zur Entwicklungszeit nicht unbedingt bekannt. Um auf die vielfältigen Situationen, die sich zur Laufzeit ergeben können und die zur Entwicklungszeit möglicherweise unbekannt sind, zu reagieren, ist eine automatische Entscheidungsfindung und Adaption zur Laufzeit notwendig [20].

Die rechte Seite von Abb. 2 zeigt, dass aufgrund der Charakteristika der Fog-Geräte nicht pauschal alle Sicherheitstechniken eingesetzt werden können. Existierende Sicherheitstechniken, die zum Schutz sensibler Daten eingesetzt werden können, haben spezifische Ressourcen-Anforderungen. Ein Beispiel ist vollhomomorphe Verschlüsselung, ein vielversprechender Ansatz aus der Kryptografie. Vollhomomorphe Verschlüsselung erlaubt es, den Chiffretext so zu bearbeiten, dass dadurch eine gewünschte Operation am Klartext durchgeführt wird – ohne dass dazu der Klartext erforderlich wäre [25]. Dadurch ermöglicht vollhomomorphe Verschlüsselung die sichere Auslagerung von Berechnungen mit sensiblen aber verschlüsselten Daten an nicht vertrauenswürdige Edge-Ressourcen. Da die Edge-Ressource in diesem Fall nur mit verschlüsselten Daten arbeitet, kann sie den Klartext nicht missbrauchen. Vollhomomorphe Verschlüsselung ist aber mit einem hohen Performanz-Overhead behaftet [26], was insbesondere bei ressourcenschwachen Geräten untragbar sein kann. Ein anderes Beispiel ist die Nutzung von sicheren Hardware-Enklaven, d. h. von Spezialhardware, die Speicherbereiche vor unbefugten Zugriffen seitens anderer Nutzer oder sogar des Betreibers schützen kann [4]. Der Einsatz sicherer Hardware-Enklaven erfordert entsprechende Spezial-CPUs. Solche CPUs sind nicht notwendigerweise auf allen Fog-Geräten verfügbar.

Aus oben genannten Gründen sollten verschiedene Datenschutzmechanismen in situativer Weise miteinander kombiniert werden. Einzelne Datenschutzmechanismen sollten je nach Bedarf aktiviert werden, so dass ihre negative Auswirkung auf Performanz und Ressourcenbedarf minimiert wird. In jeder Situation sollte jene Datenschutztechnik gewählt werden, die in Anbetracht der Kritikalität der Daten und der aktuellen Konfiguration des Fog-Systems geeignet ist.

Ein typisches Beispiel für den situativen Datenschutz liefert folgendes Szenario. Eine Berechnungsaufgabe soll von einem Endgerät an eine Edge-Ressource ausgelagert werden. Um die Auswirkungen und Risiken bezüglich Datenschutz einzuschätzen, müssen z. B. folgende Fragen geklärt werden:

- Kann dem Anbieter der Edge-Ressource vertraut werden (z. B. basierend auf vorherigen Erfahrungen mit dem Anbieter oder auf seiner Reputation in öffentlich zugänglichen Bewertungen)?
- Welche Sicherheitstechniken werden durch die Edge-Ressource unterstützt?
- Welche Daten sollen an die Edge-Ressource übergeben werden und wie sensibel sind diese Daten?
- Welchen Effekt hätten die verfügbaren Datenschutzmechanismen hinsichtlich Performanz und Kosten?

Auf Basis dieser Informationen kann eine Entscheidung über die zu nutzenden Datenschutzmechanismen getroffen werden. Abb. 3 zeigt einen beispielhaften Entscheidungsbaum. Wenn die Daten nicht sensibel sind und/oder der Anbieter vertrauenswürdig ist, kann die Berechnungsaufgabe ohne den Einsatz weiterer Datenschutzmechanismen ausgelagert werden. Andernfalls, wenn die Edge-Ressource sichere Hardware-Enklaven unterstützt, kann die Berechnungsaufgabe in einer solchen Hardware-Enklave durchgeführt werden. Wenn das nicht möglich ist, aber die Ressourcensituation es erlaubt, kann vollhomomorphe Verschlüsselung verwendet werden. Wenn keine dieser Möglichkeiten zutrifft, sollte die Berechnungsaufgabe nicht ausgelagert werden, da die damit verbundenen Datenschutzrisiken zu hoch wären. (Das Beispiel könnte natürlich noch mit weiteren Datenschutzmechanismen ergänzt werden.)

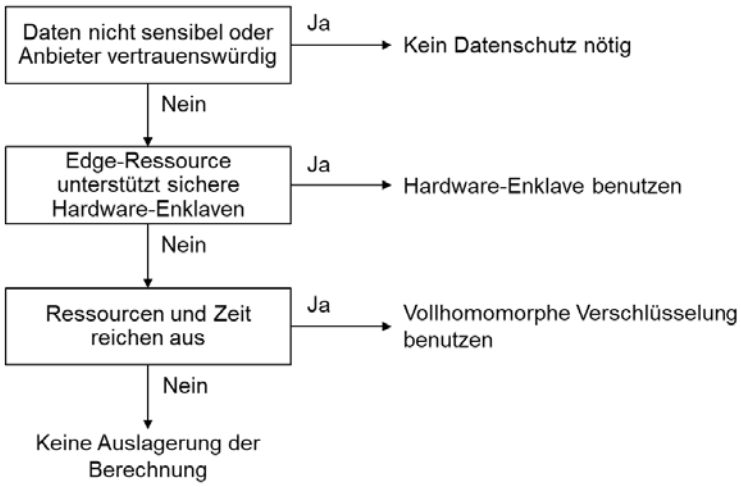

Abb. 3: Beispielhafter Entscheidungsbaum für die situative Auswahl verschiedener Datenschutzmechanismen zur Laufzeit für die Auslagerung einer Berechnungsaufgabe von einem Endgerät an eine Edge-Ressource

Forschungsfragen beim situativen Datenschutz

Einen Ansatz zur Realisierung des situativen Datenschutzes bietet das Prinzip der adaptiven Systeme. Ein adaptives System passt sich während des Betriebs selbstständig an geänderte Umgebungssituationen an. Adaptive Systeme werden in der Informatik schon länger erfolgreich eingesetzt [5][8][9][19]. Im Cloud-Computing wird zum Beispiel mittels Adaptionen erreicht, dass Ressourcen effizient, der aktuellen Situation entsprechend, eingesetzt werden, indem das System zwischen Performanz- und Kostenzielen optimal balanciert [10][11]. Man kann daher auf eine umfangreiche Menge von Methoden, Techniken und Werkzeugen als Basis für den situativen Datenschutz zurückgreifen. Situativer Datenschutz für Fog-Computing ist in gewissen Aspekten jedoch deutlich anders als das bekannte adaptive Ressourcenmanagement im Cloud-Computing, weshalb sich neue Forschungsfragen ergeben.

Ein wichtiger Unterschied bezieht sich auf den Gegenstand der Adaption. Beim adaptiven Ressourcenmanagement im Cloud-Computing wird primär die Infrastruktur eines Cloud-Anbieters adaptiert. Adaptionen im Fog-Computing betreffen verteilte Ressourcen, die oft durch unterschiedliche Anbieter betrieben werden [27]. Die Synchronisation zwischen Adaptionen, die von unabhängigen Anbietern betriebenen Ressourcen betreffen, ist dabei sowohl technisch (wegen der Integration heterogener Systeme) als auch wirtschaftlich (wegen der unterschiedlichen Anreize der Akteure) schwierig.

Erschwerend kommt hinzu, dass situativer Datenschutz über die Adaption der Infrastruktur hinausgeht und auch Adaption der Anwendungen benötigt, etwa um ein Verschlüsselungsverfahren in der Anwendung zu aktivieren oder zu deaktivieren (wie im obigen Beispiel). Zudem müssen auch die Adaptionen der Anwendung und die der Infrastruktur miteinander synchronisiert werden: z. B. kann eine Umverteilung des Software-Codes und der Daten auf andere Fog-Geräte erst dann stattfinden, wenn bis dahin die Verschlüsselung aktiviert wurde. Die Synchronisation der Adaptionen in Anwendungen und in der Infrastruktur ist eine Herausforderung, weil Anwendungen und

die Infrastruktur unabhängige Lebenszyklen haben, die ansonsten eine Entkopplung dieser Ebenen sinnvoll machen.

Ein anderer Unterschied ergibt sich aus den unterschiedlichen Zielen der Adaption. Um Performanz zu erhöhen oder Kosten zu senken, hat man beim adaptiven Ressourcenmanagement im Cloud-Computing relativ einfache Hebel: Durch Erhöhung der einem Dienst zugeteilten Ressourcen kann die Performanz in der Regel verbessert werden (unter Erhöhung der Kosten); durch Reduktion der zugeteilten Ressourcen können Kosten eingespart werden (unter Verschlechterung der Performanz). Beim Datenschutz gibt es keine so einfachen Hebel, die Risiken zu reduzieren, weil die Risiken typischerweise nicht lokaler Natur sind, sondern sich aus dem komplexen Zusammenspiel vieler Komponenten ergeben [12][16]. Auch der effektive Einsatz von Risikominderungsverfahren erfordert oft das koordinierte Ändern vieler Komponenten [21].

Schließlich sind herkömmliche Adaptionsmechanismen, wie wir sie aus dem Cloud-Ressourcenmanagement kennen, meist reaktiv. Sie reagieren auf Änderungen, nachdem diese festgestellt wurden. Wenn z. B. beobachtet wird, dass die Last eines Cloud-Dienstes zunimmt, können automatisch mehr Ressourcen zugeteilt werden, um die Lastspitze abzufangen. Dabei kann es vorkommen, dass gewisse Anforderungen, etwa eine obere Schranke für die Antwortzeit des Dienstes, vorübergehend verletzt werden, bevor die Adaption wieder die Erfüllung der Anforderung sicherstellt. Bei Performanz oder Kosten ist eine solche temporäre Verletzung der Anforderungen oft tolerierbar. Bei Datenschutz als Adaptionsziel ist das anders: Schon eine vorübergehende Verletzung von Datenschutzanforderungen kann irreversible Folgen haben. Wenn eine böswillige Partei unerlaubt Zugriff auf sensible Daten bekommen hat, hilft es möglicherweise nicht mehr, wenn der Zugriff später entzogen wird, denn der Angreifer kann bis dahin eine Kopie der Daten erstellt haben, die er dann missbrauchen kann. Das heißt, dass situativer Datenschutz nicht reaktiv, sondern proaktiv sein muss: Gefährliche Konfigurationen des Fog-Systems müssen vermieden werden.

Um situativen Datenschutz zu verwirklichen, sind somit eine Reihe von Forschungsfragen zu adressieren. Diese Forschungsfragen umfassen:

- Was sind geeignete Modellierungskonzepte und Modellierungssprachen (analog z. B. zu [13][7]), mit denen alle für den Datenschutz wichtigen Aspekte von Fog-Systemen erfasst werden können, um eine automatische Analyse der Modelle und somit eine dynamische Entscheidungsfindung zur Laufzeit zu ermöglichen?
- Was sind realistische Vertrauens- und Angriffsmodelle im Fog-Computing, und wie können diese Modelle bei automatischen Entscheidungen zur Laufzeit berücksichtigt werden?
- Wie kann man Fog-Systeme effektiv und effizient beobachten (analog z. B. zu [20]), um z. B. die konkrete Verteilung des Software-Codes zu erkennen?
- Wie kann eine automatische Risikoanalyse von Fog-Systemen algorithmisch gelöst werden?
- Wie kann eine optimale Entscheidungsfindung auf den verschiedenen Ebenen des Fog-Computing (Endgeräte, Edge-Ressourcen, Cloud) algorithmisch umgesetzt werden?
- Wie kann die Effizienz und Skalierbarkeit dieser Algorithmen erreicht werden, damit Adaptionen auch bei schnellen Änderungen der Umgebung in Echtzeit beschlossen und ausgeführt werden können?
- Wie kann die korrekte Funktionsweise situativer Datenschutzlösungen gesichert werden (z. B. durch Methoden zur Verifikation, Test und Audit)?
- Wie kann das Zusammenspiel mehrerer Systeme, die sich alle potenziell selbst adaptieren, koordiniert und synchronisiert werden?

Fazit

Der Schutz sensibler Daten im Fog-Computing ist ein wichtiges Problem. Schon im Cloud-Computing ist es schwierig, den Datenschutz zu gewährleisten; die zusätzliche Komplexität und vielfältige Dynamik von Fog-Systemen macht diese Aufgabe noch schwieriger. In diesem Beitrag haben wir argumentiert, dass verschiedene Datenschutztechniken auf situative Weise miteinander kombiniert werden sollten, um die spezifischen Herausforderungen beim Datenschutz in der Fog zu adressieren. Zuletzt haben wir relevante Forschungsfragen dargelegt, die es zu beantworten gilt, um einen solchen situativen Datenschutz zu ermöglichen.

Danksagung

Die vorgestellten Forschungsarbeiten werden gefördert im Rahmen des EU Horizont-2020 Forschungs- und Innovationsprogramms unter Förderkennzeichen 731678 (RestAssured), sowie von der DFG im Rahmen des Schwerpunktprogramms SPP1593: „Design For Future – Managed Software Evolution“ unter Förderkennzeichen PO 607/3-2 (iObserve).

Literatur

[1] A. Alrawais, A. Alhothaily, C. Hu, X. Cheng. Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, March / April 2017, pp. 34-42, 2017
[2] A. Aral, I. Brandic. Quality of Service channelling for latency sensitive edge applications. IEEE International Conference on Edge Computing, pp. 166-173, 2017
[3] C. A. Ardagna, R. Asal, E. Damiani, Q. H. Vu. From security to assurance in the cloud: A survey. ACM Computing Surveys, 48(1): art. 2, 2015
[4] V. Costan, I. A. Lebedev, S. Devadas. Sanctum: Minimal hardware extensions for strong software isolation. USENIX Security Symposium, pp. 857-874, 2016
[5] E. Di Nitto, C. Ghezzi, A. Metzger, M. Papazoglou, K. Pohl. A journey to highly dynamic, self-adaptive service-based applications. Automated Software Engineering, 15(3-4):313-341, 2008
[6] T. He, E. N. Ciftcioglu, S. Wang, K. S. Chan. Location privacy in mobile edge clouds: A chaff-based approach. IEEE Journal on Selected Areas in Communications, 35(11):2625-2636, 2017
[7] R. Heinrich, R. Jung, E. Schmieders, A. Metzger, W. Hasselbring, R. Reussner, K. Pohl, Architectural run-time models for operator-in-the-loop adaptation of cloud applications. IEEE 9th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Environments, pp. 36-40, 2015
[8] J. O. Kephart, D. M. Chess. The vision of autonomic computing. Computer, 36(1):41-50, 2003
[9] M. Luthra, B. Koldehofe, P. Weisenburger, G. Salvaneschi. TCEP: Adapting to dynamic user environment by enabling transitions between operator placement mechanisms. 12th ACM International Conference on Distributed and Event-based Systems, pp. 136-147, 2018
[10] Z. Á. Mann. Multicore-aware virtual machine placement in cloud data centers. IEEE Transactions on Computers, 65(11):3357-3369, 2016
[11] Z. Á. Mann, A. Metzger. Optimized cloud deployment of multi-tenant software considering data protection concerns. 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 609-618, 2017
[12] Z. Á. Mann, A. Metzger. The special case of data protection and self-adaptation. ACM/IEEE 13th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, pp. 190-191, 2018
[13] Z. Á. Mann, A. Metzger, S. Schoenen. Towards a run-time model for data protection in the cloud. I. Schaefer, D. Karagiannis, A. Vogelsang, D. Méndez, C. Seidl (Hrsg.): Modellierung 2018, pp. 71-86. Gesellschaft für Informatik e.V., 2018
[14] F. Mattern, C. Floerkemeier. Vom Internet der Computer zum Internet der Dinge. Informatik-Spektrum 33(2):107-121, 2010
[15] G. Orsini, D. Bade, W. Lamersdorf. CloudAware: A context-adaptive middleware for mobile edge and cloud computing applications. IEEE International Workshops on Foundations and Applications of Self* Systems, pp. 216-221, 2016
[16] A. Palm, Z. Á. Mann, A. Metzger. Modeling data protection vulnerabilities of cloud systems using risk patterns. 10th System Analysis and Modeling Conference, pp. 1-19, 2018
[17] Z. Riaz, F. Dürr, K. Rothermel. On the privacy of frequently visited user locations. 17th IEEE International Conference on Mobile Data Management, vol. 1, pp. 282-291, 2016
[18] B. Richerzhagen, B. Koldehofe, R. Steinmetz. Immense dynamism. German Research 2/2015, 24-27, WILEY-VCH, 2015
[19] M. Salehie, L. Tahvildari. Self-adaptive software: Landscape and research challenges. ACM Transactions on Autonomous and Adaptive Systems, 4(2): art. 14, 2009
[20] E. Schmieders, A. Metzger, K. Pohl. Runtime model-based privacy checks of big data cloud services. International Conference on Service-Oriented Computing, pp. 71-86, 2015
[21] S. Schoenen, Z. Á. Mann, A. Metzger. Using risk patterns to identify violations of data protection policies in cloud systems. Braubach L. et al. (eds): Service-Oriented Computing – ICSOC 2017 Workshops, LNCS vol. 10797, pp. 296-307, 2018
[22] O. Skarlat, S. Schulte, M. Borkowski, P. Leitner. Resource provisioning for IoT services in the fog. IEEE 9th International Conference on Service-Oriented Computing and Applications, 32-39, 2016

[23] I. Stojmenovic, S. Wen. The fog computing paradigm: Scenarios and security issues. Federated Conference on Computer Science and Information Systems, 1-8, 2014
[24] V. Tietz, G. Blichmann, G. Hübsch. Cloud-Entwicklungsmethoden. Informatik-Spektrum, 34(4):345-354, 2011
[25] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan. Fully homomorphic encryption over the integers. Advances in Cryptology – EUROCRYPT 2010, LNCS vol. 6110, pp. 24-43, 2010
[26] W. Wang, Y. Hu, L. Chen, X. Huang, B. Sunar. Exploring the feasibility of fully homomorphic encryption. IEEE Transactions on Computers, 64(3): 698-706, 2015
[27] L. Wang, L. Jiao, J. Li, M. Mühlhäuser. Online resource allocation for arbitrary user mobility in distributed edge clouds. IEEE 37th International Conference on Distributed Computing Systems, pp. 1281-1290, 2017
[28] S. Wrobel, H. Voss, J. Köhler, U. Beyer, S. Auer. Big Data, Big Opportunities. Informatik-Spektrum 38(5): 370-378, 2015
[29] S. Yi, C. Li, Q. Li. A survey of fog computing: Concepts, applications and issues. Workshop on Mobile Big Data, 37-42, 2015
[30] S. Yi, Z. Qin, Q. Li. Security and privacy issues of fog computing: A survey. International Conference on Wireless Algorithms, Systems, and Applications, 685-695, 2015