Karlsruher Institut für Technologie

**Institut für Angewandte Informatik
und Formale Beschreibungsverfahren**

CRITICAL INFORMATION INFRASTRUCTURES

KIT | Institut AIFB | Postfach 6980 | 76049 Karlsruhe

Prof. Dr. Ali Sunyaev

Kaiserstraße 89
76133 Karlsruhe

Telefon: 0721 608-46037
Fax: 0721 608-46581
E-Mail: sunyaev@kit.edu
Web: http://cii.aifb.kit.edu

An alle Bachelor-Studierenden der Studiengänge
Wirtschaftsingenieurwesen und
Informationswirtschaft

Datum: 15. Oktober 2019

Zertifikat seit 2010 audit familiengerechte hochschule

Exklusiver Austausch mit der Yale University!

Die Forschungsgruppe Critical Information Infrastructure (cii) von Prof. Dr. Ali Sunyaev am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) (http://cii.aifb.kit.edu) bietet im Rahmen des DAAD RISE Austauschprogramms die einzigartige Möglichkeit, ein mehrmonatiges Praktikum an der Yale University bei Prof. Jakub Szefer im Computer Architecture and Security Lab (http://caslab.csl.yale.edu/) durchzuführen.

Die Nachfrage nach Wissenschaftlern sowie Ingenieuren mit internationaler Erfahrung ist in Wirtschaft und Forschung stark gestiegen. Mit RISE Weltweit unterstützt der DAAD den internationalen Austausch in den Natur- und Ingenieurwissenschaften. Deutsche Bachelorstudierende erhalten ein Stipendium für ein Praktikum in den verschiedensten Ländern der Welt und werden von Forschern vor Ort betreut. RISE steht für Research Internships in Science and Engineering. RISE Weltweit finanziert sich aus Mitteln des Bundesministeriums für Bildung und Forschung. Weiterführende Informationen und FAQs sind unter https://www.daad.de/rise/de/rise-weltweit/ zu finden.

Die Praktikanten werden durch jeweils einen Doktoranden der Forschungsgruppe cii am KIT und des Teams von Prof. Szefer an der Yale Universität gemeinsam geführt und unterstützen den Lehrstuhl bei aktuellen (experimentellen) Arbeiten in der Forschung. Bei der thematischen Ausgestaltung wird hierbei Rücksicht auf das Interesse und die Fähigkeiten des jeweiligen Studierenden genommen, sodass eine persönliche Weiterentwicklung erzielt werden kann. In den vergangenen Jahren haben bereits sechs Studierende an dem Austausch erfolgreich teilgenommen – so dass hier auf direkte Erfahrungen gerne zurückgegriffen werden kann. Zudem sind auch wissenschaftliche Publikationen der Studierenden, gemeinsam mit den Doktoranden und Professoren entstanden.

Themenschwerpunkte:

- Cloud Computing
- Automatisierte Zertifizierung von IT-Systemen
- Artificial Intelligence und Maschine Learning
- Blockchain und Distributed Ledger Technologien
- und weitere spannende aktuelle Themengebiete

Besucheranschrift:
Karlsruher Institut für Technologie
Institut AIFB
Kaiserstr. 89, Geb. 05.20
76133 Karlsruhe

Postanschrift:
Karlsruher Institut für Technologie
Institut AIFB
Postfach 6980
76049 Karlsruhe

Karlsruher Institut für Technologie

Wir bieten:

- Ein Aufenthalt an der Yale University mit enger Integration in das Team von Prof. Szefer
- Spannende Forschungsthemen zur eigenständigen Bearbeitung im Rahmen des Praktikums
- Viel Freiraum zum Erkunden der Yale University und der USA
- Der DAAD vergibt im Rahmen seines DAAD RISE Programms ein Stipendium, das Folgendes beinhaltet:
    - ein monatliches Vollstipendium (Stipendienrate von monatlich **1050,- EUR**)
    - eine Reisekostenpauschale
    - Kranken-, Unfall- und Haftpflichtversicherung

Voraussetzungen:

- Nur **vollimmatrikulierte Bachelor-Studierende** in den Studiengängen **Wirtschaftsingenieurwesen, Informationswirtschaft, Informatik,** oder **Elektro- und Informationstechnik**
- Für Master-Studierenden gibt es leider kein ähnliches Angebot zurzeit!
- Studierender befindet sich im letzten Drittel seines Bachelorstudiums. Es sollte dem Studierenden daher möglich sein, vor Beginn des Praktikums eine Bachelorarbeit an unserer Forschungsgruppe schreiben.
- Die Praktika dauern zwischen sechs Wochen und drei Monaten (Die Laufzeit des Praktikums wird individuell zwischen dem Praktikanten und dem Lehrstuhl vereinbart)
- Frühester Start des Praktikums ist der **1. Juni 2020.** Das Praktikum sollte möglichst in der vorlesungsfreien Zeit stattfinden.
- Spätester Laufzeitbeginn ist der **15. September** und spätestes Laufzeitende des Stipendiums immer der **31. Oktober** (für Oktober ist dann eine Einschreibebestätigung nötig, die im Sommer nachgereicht werden muss). **Hinweis:** Stipendiaten, die nicht mehr im WS nach dem Praktikum in einem Bachelorstudiengang eingeschrieben sind, müssen das Praktikum spätestens zum 15. Oktober beenden.
- Es ist kein Mindestnotendurchschnitt erforderlich, jedoch nimmt der Notendurchschnitt eine wichtige Rolle bei der Platzierung und Stipendienvergabe durch den DAAD ein.
- Nach dem Gemeinsamen Europäischen Referenzrahmen (GER) sollten die Englischkenntnisse auf Stufe B2 sein und mit einem anerkannten Sprachzertifikat nachgewiesen werden
    - Bspw. Cambridge (FCE, CAE, CPE), IELTS, TELC, TOEFL, TOEIC, OLS
    - Sprachzertifikate dürfen nicht älter als zwei Jahre sein
    - Bei Rückfragen bzgl. des Sprachzertifikats muss sich immer an den DAAD gewendet werden
- Der Studierende sollte **im Vorfeld eine Seminar- oder Bachelorarbeit bei der Forschungsgruppe cii** schreiben, um sich bereits inhaltlich auf den Austausch vorzubereiten.

Bewerbungsfrist:

- Die Bewerbung muss bis einschließlich **1. November 2019** am Lehrstuhl bei Sebastian Lins (sebastian.lins@kit.edu) in Englischer Sprache elektronisch eingehen (Motivationsschreiben, CV und aktueller Notenauszug).
- Der Lehrstuhl nimmt eine Vorauswahl der Studierenden vor, sodass sich **maximal 2 Studierende pro Jahr** im Rahmen des DAAD RISE Programms für einen Austausch bei Prof. Szefer bewerben können
- Die **endgültige Auswahl erfolgt im DAAD**. Alle Bewerber werden bis Mitte März 2020 über das Auswahlergebnis informiert.

Ansprechpartner für Rückfragen:

M. Sc. Sebastian Lins, sebastian.lins@kit.edu, 0721 608-42819, http://cii.aifb.kit.edu/, Raum: 2B-05.2 (Gebäude: 05.20)

Democratizing Machine Learning: Toward a Secure, Distributed, and Powerful Computer

Background

Machine learning (ML) has shown tremendous capabilities in various application domains over the past few years. An example of such an application domain is genomics, where ML can be applied to human gene expressions to predict certain disease therapy success rates. Thus, the application of ML in genomics has the potential to strongly improve cure rates while increasing health care cost-efficiency.

As single entities and software engineers often do not have the data, computing resources, or expertise to build their own ML models, Machine Learning as a Service (MLaaS) is emerging. MLaaS refers to an organization (i.e., the MLaaS provider) that offers to run an ML model on a cloud platform (e.g., Amazon Web Services, Microsoft Azure, Google Cloud). A client can then upload data to the cloud server, where the server then runs the MLaaS model with that client's data and returns the result to the client (e.g., a doctor uploads gene data to the cloud and, after an ML model runs there, it returns a result to the doctor of how successful certain therapies are predicted to be). However, several trust issues exist in this scenario, especially with sensitive data such as gene data. How can a doctor be certain that the MLaaS provider or the cloud company handles the data securely and does not abuse the data? How can the patient be sure of that? And how can the MLaaS provider be sure that the cloud company handles its models and its customers' data securely?

Trusted execution environments (TEEs) present themselves as a promising solution for those trust issues. A TEE is a secure area in a CPU, which performs computations while guaranteeing integrity and data confidentiality. In the described scenario, the cloud provider would, for example, sell TEE computing resources. The MLaaS provider then rents these resources and has a machine learning model ready for inference. The client (e.g., a doctor) can then run the service inside the TEE and use cryptographic techniques to ensure that nobody else can see the raw data or the result. Thus, the system provides stronger data confidentiality guarantees and has a higher chance of user acceptance.

Going even further, Blockchain technology can be used in the presented scenario to create new marketplaces for data, TEE resources, or machine learning models to be traded. Such a system has the potential to strongly increase health care quality while keeping cost low.

The goal of this research project is to implement ML algorithms in a TEE. Data from the health care and genomics domain can be used for it, however, the student may also propose other application domains. As this is a broad umbrella topic, a specific topic will be designed based on the student's interest and skills. Further areas where the student can focus on, are system security analysis, or blockchain-enabled data, resource, and model marketplaces. The ideal candidate has good programming skills as well as a solid understanding of hardware architectures and machine learning. Knowledge in TEEs and Blockchains is nice to have, but not necessary. The work allows you to gain deep knowledge and experience in rapidly growing fields: trusted hardware, machine learning, blockchain, and digital health.

Possible tasks

- Design, implementation, and evaluation of ML algorithms on a TEE (e.g., Neural Networks on Intel SGX)
- Design, implementation, and evaluation of blockchain-based marketplaces (e.g., for data, model, and TEE resource trading)
- Analysis of an integrated system incorporating security, privacy, and economic aspects

Introductory literature

Hynes, Nick; Dao, David; Yan, David; Cheng, Raymond; Song, Dawn (2018): A demonstration of sterling: a privacy-preserving data marketplace. In *Proceedings of the VLDB Endowment* 11 (12), pp. 2086–2089. Available online at http://www.vldb.org/pvldb/vol11/p2086-hynes.pdf.

Jones, Michael; Johnson, Matthew; Shervey, Mark; Dudley, Joel T.; Zimmerman, Noah (2019): Privacy-Preserving Methods for Feature Engineering Using Blockchain: Review, Evaluation, and Proof of Concept. In *Journal of medical Internet research* 21 (8), e13600. Available online at https://www.jmir.org/2019/8/e13600/pdf.

Kunkel, Roland; Le Quoc, Do; Gregor, Franz; Arnautov, Sergei; Bhatotia, Pramod; Fetzer, Christof (2019): TensorSCONE: A Secure TensorFlow Framework using Intel SGX. In *arXiv preprint arXiv:1902.04413*. Available online at https://arxiv.org/pdf/1902.04413.pdf.

Noah Johnson (Ed.) (2019): Building a Secure Data Market on Blockchain. Burlingame, CA: USENIX Association. Available online at https://www.usenix.org/conference/enigma2019/presentation/song.

Tramer, Florian; Boneh, Dan (2018): Slalom: Fast, verifiable and private execution of neural networks in trusted hardware. In *arXiv preprint arXiv:1806.03287*. Available online at https://arxiv.org/pdf/1806.03287.pdf.

Making the Cloud a Secure Place: Toward Secure Service Certifications for Complex Cloud Infrastructures

Background

Security breaches of cloud services continue to make headlines in the media. Recent reports show that 2019 is likely to become the worst year so far concerning the number of data breaches. Common security issues include attacks from insiders and technical system vulnerabilities that open up possibilities for all kinds of malicious attacks. Such developments make consumers of cloud services worry about what is going on at their cloud service provider. Consumers mandate high levels of assurances from cloud service providers making sure that their data is safe and secured.

Continuous service certification (CSC) is a valuable means for cloud service providers to deliver on that promise. CSC follows the general concept of certification that online customers often encounter in e-commerce shops (e.g., TRUSTe, VeriSign, or BBBOnline). CSC builds on this concept by focusing on ways to provide continuous assurances of important properties of the cloud infrastructure to customers (e.g., availability, security, or privacy). One approach to realizing CSC is *monitoring-based CSC*. In monitoring-based CSC, autonomous systems collect, aggregate, and analyze audit-relevant monitoring data from the cloud infrastructure. Such systems then provide evidence to a third-party auditor who assesses the evidence before issuing the certification to the cloud service provider.

This approach has several benefits for consumers and cloud service providers alike. It allows service certifications to provide continuous assurances based on up-to-date monitoring data from the cloud infrastructure. Today's certification schemes have typical validity periods from one year until three years. CSC can reduce this time, increasing the accuracy of assurance claims made by service certifications. Besides, CSC can help reduce errors and provide valuable insights into managing complex cloud environments.

However, the scientific debate on these systems continues to be conceptual, with few researchers and cloud service providers seeking to implement such systems in practice. One major barrier to implementing these systems in practice is the lack of design knowledge and guidelines.

This research project looks at one critical issue of CSC to help bring this concept closer to practical reality, which is making sure that cloud service providers can protect monitoring systems from malicious actions by insiders and outsiders. Protecting the integrity of these systems and ensuring the reliability of monitoring data is paramount to build confidence and trust in such systems in practice. Researchers and cloud service providers need further research to gain insights into how cloud service providers can protect these systems. To address this pressing gap in research, this research project seeks to answer the following research questions (RQ):

RQ1: *What are potential attack vectors of monitoring systems that seek to enable continuous certification of cloud services?*

RQ2: *How can cloud service providers design monitoring systems that reduce or eradicate the risks from these attacks?*

Research approach

The approach to address these research questions follows a design science research paradigm as an overarching methodological foundation. The project will ask students to synthesize approaches to protect CSC monitoring systems from malicious actions by insiders and outsiders. Students will examine and derive concrete enhancements to the architecture of CSC monitoring systems and implement a prototype to test the proposed enhancements.

The project will follow a three-step approach. The first step is to synthesize extant knowledge from the literature into attacks on such systems and how to mitigate those attacks. This step will require students to conduct a systematic literature review. The result is an in-depth understanding of the knowledge base relevant to the topic.

The second step is to derive tentative design knowledge based on insights from the literature. For instance, the use of cryptographic methods can be a valuable direction for making CSC monitoring systems more secure, which is so far unexplored in extant research. The result is a set of tentative design principles that can guide practical implementations of such systems.

The last step involves testing and refining these tentative design principles in close collaboration with experts from Yale University. Students will test the derived design principles and recommendations by developing a prototype.

Possible prospective tasks of the intern

Following the approach outlined above, the intern will pursue the following tasks:

- Derive a set of testable design principles for improving CSC monitoring systems' security based on relevant scientific research
- Test and refine selected design principles using a prototyping approach
- Work on the project in close collaboration with experts on the topic
- Derive practical guidance for cloud service providers that help them develop monitoring systems for complex cloud infrastructures that satisfy high standards of security and safety and also help to deliver more secure cloud services to consumers