Topics Seminar System Administration

Updated: November 27, 2019

Jörg Cassens

Seminar Medieninformatik
Winter Term 2019/2020

medieninformatik
IMAI – Institut für Mathematik und Angewandte Informatik

Topics

A list of texts not assigned yet can be found on on page 6.

10. **Systemadministration**
(für das Gebiet Systemadministration und Internet-Technologien)

10.1. **Survey: Internet of Things**

□ **Topic not assigned**

▷ Paper: Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things – A survey of topics and trends. Information Systems Frontiers, 17(2), 261-274.
Download paper
Abstract: *The Internet of Things is a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective. Ultimately, IoT devices will be ubiquitous, context-aware and will enable ambient intelligence. This article reports on the current state of research on the Internet of Things by examining the literature, identifying current trends, describing challenges that threaten IoT diffusion, presenting open research questions and future directions and compiling a comprehensive reference list to assist researchers.*

10.2. **Survey: Middleware for Internet of Things**

□ **Topic not assigned**

▷ Paper: Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for internet of things: a survey. IEEE Internet of Things Journal, 3(1), 70-95.
Download paper
Abstract: *The Internet of Things (IoT) envisages a future in which digital and physical things or objects (e.g., smartphones, TVs, cars) can be connected by means of suitable information and communication technologies, to enable a range of applications and services. The IoT's characteristics, including an ultra-large- scale network of things, device and network level heterogeneity, and large numbers of events generated spontaneously by these things, will make development of the diverse applications and services a very challenging task. In general, middleware can ease a development process by integrating heterogeneous computing and communications devices, and supporting interoperability within the diverse applications and services. Recently, there have been a number of proposals for IoT middleware. These proposals mostly addressed wireless sensor networks (WSNs), a key component of IoT, but do not consider RF identification (RFID), machine-to- machine (M2M) communications, and supervisory control and data acquisition (SCADA), other three core elements in the IoT vision. In this paper, we outline a set of requirements for IoT middleware, and present a comprehensive review of the exist- ing middleware solutions against those requirements. In addition, open research issues, challenges, and future research directions are highlighted.*

10.3. Survey: Security for the Internet of Things

□ **Topic not assigned**

▷ Paper: J Granjal, E Monteiro, JS Silva: Security for the internet of things: a survey of existing protocols and open research issues. In: IEEE Communications Surveys & Tutorials, Volume: 17, Issue: 3, thirdquarter 2015, pp 1294-1312.
Download paper
Abstract: *The Internet of Things (IoT) introduces a vision of a future Internet where users, computing systems, and everyday objects possessing sensing and actuating capabilities cooperate with unprecedented convenience and economical benefits. As with the current Internet architecture, IP-based communication protocols will play a key role in enabling the ubiquitous connectivity of devices in the context of IoT applications. Such communication technologies are being developed in line with the constraints of the sensing platforms likely to be employed by IoT applications, forming a communications stack able to provide the required power-efficiency, reliability, and Internet connectivity. As security will be a fundamental enabling factor of most IoT applications, mechanisms must also be designed to protect communications enabled by such technologies. This survey analyzes existing protocols and mechanisms to secure communications in the IoT, as well as open research issues. We analyze how existing approaches ensure fundamental security requirements and protect communications on the IoT, together with the open challenges and strategies for future research work in the area. This is, as far as our knowledge goes, the first survey with such goals.*

10.4. Security Considerations for Cloud-Supported IoT

□ **Topic not assigned**

▷ Paper: Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269-284.
Download paper
Abstract: *To realise the broad vision of pervasive computing, underpinned by the "Internet of Things" (IoT), it is essential to break down application and technology-based silos and support broad connectivity and data sharing; the cloud being a natural enabler. Work in IoT tends towards the subsystem, often focusing on particular technical concerns or application domains, before offloading data to the cloud. As such, there has been little regard given to the security, privacy and personal safety risks that arise beyond these subsystems; that is, from the wide-scale, cross- platform openness that cloud services bring to IoT. In this paper we focus on security considerations for IoT from the perspectives of cloud tenants, end-users and cloud providers, in the context of wide-scale IoT proliferation, working across the range of IoT technologies (be they things or entire IoT subsystems). Our contribution is to analyse the current state of cloud-supported IoT to make explicit the security considerations that require further work.*

10.5. Internet of Things Security & Privacy

☒ **Presented by: Constantin Bettels**

▷ Paper: Dabbagh, M., & Rayes, A. (2017). Internet of Things Security and Privacy. In Internet of Things From Hype to Reality (pp. 195-223). Springer International Publishing.
Download paper
Abstract: *The Internet of Things (IoT) promises to make our lives more convenient by turning each physical object in our surrounding environment into a smart object that can sense the environment, communicate with the remaining smart objects, perform reasoning, and respond properly to changes in the surrounding environment. However, the conveniences that the IoT brings are also associated with new security risks and privacy issues that must be addressed properly. Ignoring these security and privacy issues will have serious effects on the different aspects of our lives including the homes we live in, the cars we ride to work, and even the effects will reach our own bodies.*

10.6. Security and Quality Aware Architecture for IoT

□ **Topic not assigned**

▷ Paper: Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. Information Systems Frontiers, 18(4), 665-677.
Download paper
Abstract: *Internet of Things (IoT) is characterized, at the system level, by high diversity with respect to enabling tech- nologies and supported services. IoT also assumes to deal with a huge amount of heterogeneous data generated by devices, transmitted by the underpinning infrastructure and processed to support value-added services. In order to provide users with valuable output, the IoT architecture should guarantee the suitability and trustworthiness of the processed data. This is a major requirement of such systems in order to guarantee robustness and reliability at the service level. In this paper, we introduce a novel IoT architecture able to support security, privacy and data quality guarantees, thereby effectively boosting the diffusion of IoT services.*

10.7. Integration Cloud Computing & Internet of Things

- □ Topic not assigned
- ▷ Paper: Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56, 684-700.

  Download paper

  Abstract: *Cloud computing and Internet of Things (IoT) are two very different technologies that are both already part of our life. Their adoption and use are expected to be more and more pervasive, making them important components of the Future Internet. A novel paradigm where Cloud and IoT are merged together is foreseen as disruptive and as an enabler of a large number of application scenarios. In this paper, we focus our attention on the integration of Cloud and IoT, which is what we call the CloudIoT paradigm. Many works in literature have surveyed Cloud and IoT separately and, more precisely, their main properties, features, underlying technologies, and open issues. However, to the best of our knowledge, these works lack a detailed analysis of the new CloudIoT paradigm, which involves completely new applications, challenges, and research issues. To bridge this gap, in this paper we provide a literature survey on the integration of Cloud and IoT. Starting by analyzing the basics of both IoT and Cloud Computing, we discuss their complementarity, detailing what is currently driving to their integration. Thanks to the adoption of the CloudIoT paradigm a number of applications are gaining momentum: we provide an up-to-date picture of CloudIoT applications in literature, with a focus on their specific research challenges. These challenges are then analyzed in details to show where the main body of research is currently heading. We also discuss what is already available in terms of platforms–both proprietary and open source–and projects implementing the CloudIoT paradigm. Finally, we identify open issues and future directions in this field, which we expect to play a leading role in the landscape of the Future Internet.*

10.8. Cloud Computing Adoption Framework for Business Clouds

- □ Topic not assigned
- ▷ Paper: Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.

  Download paper

  Abstract: *This paper presents a Cloud Computing Adoption Framework (CCAF) security suitable for business clouds. CCAF multi-layered security is based on the development and integration of three major security technologies: firewall, identity management and encryption based on the development of Enterprise File Sync and Share technologies. This paper presents our motivation, related work and our views on security framework. Core technologies have been explained in details and experiments were designed to demonstrate the robustness of the CCAF multi-layered security. In penetration testing, CCAF multi-layered security could detect and block 99.95% viruses and trojans and could maintain 85% and above of blocking for 100 hours of continuous attacks. Detection and blocking took less than 0.012 second per trojan and viruses. A full CCAF multi-layered security protection could block all SQL injection providing real protection to data. CCAF multi-layered security had 100% rate of not reporting false alarm. All F-measures for CCAF test results were 99.75% and above. How CCAF multi-layered security can blend with policy, real services and blend with business activities have been illustrated. Research contributions have been justified and CCAF multi-layered security can offer added value for volume, velocity and veracity for Big Data services operated in the Cloud.*

10.9. Data Security with Cloud Computing Adoption Framework

- □ Topic not assigned
- ▷ Paper: Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on Services Computing, 9(1), 138-151.

  Download paper

  Abstract: *Offering real-time data security for petabytes of data is important for Cloud Computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. We believe this can only be able to achieve with an approach that is systematic, adoptable and well-structured. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. This paper explains the overview, rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. Since our Data Center has 10 petabytes of data, there is a huge task to provide real-time protection and quarantine. We use Business Process Modeling Notation (BPMN) to simulate how data is in use. The use of BPMN simulation allows us to evaluate the chosen security performances before actual implementation. Results show that the time to take control of security breach can take between 50 and 125 hours. This means that additional security is required to ensure all data is well-protected in the crucial 125 hours. This paper has also demonstrated that CCAF multi-layered security can protect data* *in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption. To validate CCAF, this paper has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 trojans and viruses. The CCAF multi-layered security can block 9,919 viruses and trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated. The experiments show although the percentage of blocking can decrease for continuous injection of viruses and trojans, 97.43% of them can be quarantined. Our CCAF multi-layered security has an average of 20% better performance than the single-layered approach which could only block 7,438 viruses and trojans. CCAF can be more effective when combined with BPMN simulation to evaluate security process and penetrating testing results.*

10.10. **Privacy Preserving Content-Based Image Retrieval Scheme**

□ **Topic not assigned**

▷ Paper: Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., & Ren, K. (2016). A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Transactions on Information Forensics and Security, 11(11), 2594-2608.
Download paper
Abstract: *With the increasing importance of images in people's daily life, Content-based Image Retrieval (CBIR) has been widely studied. Compared with text documents, images consume much more storage space. Hence, its maintenance is considered to be a typical example for cloud storage outsourcing. For privacy-preserving purposes, sensitive images, such as medical and personal images, need to be encrypted before outsourcing, which makes the CBIR technologies in plaintext domain to be unusable. In this paper, we propose a scheme that supports CBIR over encrypted images without leaking the sensitive information to the cloud server. Firstly, feature vectors are extracted to represent the corresponding images. After that, the pre-filter tables are constructed by locality-sensitive hashing to increase search efficiency. Moreover, the feature vectors are protected by the secure kNN algorithm, and image pixels are encrypted by a standard stream cipher. In addition, considering the case that the authorized query users may illegally copy and distribute the retrieved images to someone unauthorized, we propose a watermark-based protocol to deter such illegal distributions. In our watermark-based protocol, a unique watermark is directly embedded into the encrypted images by the cloud server before images are sent to the query user. Hence, when an illegal image copy is found, the unlawful query user who distributed the image can be traced by the watermark extraction. The security analysis and experiments show the security and efficiency of the proposed scheme*

10.11. **Intrusion Detection for Mobile Cloud Computing**

□ **Topic not assigned**

▷ Paper: Gai, K., Qiu, M., Tao, L., & Zhu, Y. (2016). Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Security and Communication Networks, 9(16), 3049-3058.
Download paper
Abstract: *Mobile cloud computing is applied in multiple industries to obtain cloud-based services by leveraging mobile technologies. With the development of the wireless networks, defending threats from wireless communications have been playing a remarkable role in the Web security domain. Intrusion detection system (IDS) is an efficient approach for protecting wireless communications in the Fifth Generation (5G) context. In this paper, we identify and summarize the main techniques being implemented in IDSs and mobile cloud computing with an analysis of the challenges for each technique. Addressing the security issue, we propose a higher level framework of implementing secure mobile cloud computing by adopting IDS techniques for applying mobile cloud-based solutions in 5G networks. On the basis of the reviews and synthesis, we conclude that the implementation of mobile cloud computing can be secured by the proposed framework because it will provide well-protected Web services and adaptable IDSs in the complicated heterogeneous 5G environment.*

10.12. **Multi-User Computation Offloading Mobile Cloud**

□ **Topic not assigned**

▷ Paper: Chen, X., Jiao, L., Li, W., & Fu, X. (2016). Efficient multi-user computation offloading for mobile-edge cloud computing. IEEE/ACM Transactions on Networking, 24(5), 2795-2808.
Download paper
Abstract: *Mobile-edge cloud computing is a new paradigm to provide cloud computing capabilities at the edge of pervasive radio access networks in close proximity to mobile users. In this paper, we first study the multi-user computation offloading problem for mobile-edge cloud computing in a multi-channel wireless interference environment. We show that it is NP-hard to compute a centralized optimal solution, and hence adopt a game theoretic approach for achieving efficient computation offloading in a distributed manner. We formulate the distributed computation offloading decision making problem among mobile device users as a multi-user computation offloading game. We analyze the structural property of the*

game and show that the game admits a Nash equilibrium and possesses the finite improvement property. We then design a distributed computation offloading algorithm that can achieve a Nash equilibrium, derive the upper bound of the convergence time, and quantify its efficiency ratio over the centralized optimal solutions in terms of two important performance metrics. We further extend our study to the scenario of multi-user computation offloading in the multi-channel wireless contention environment. Numerical results corroborate that the proposed algorithm can achieve superior computation offloading performance and scale well as the user size increases.

10.13. **Survey & Taxonomy Energy Efficient Resource Allocation**

- □ **Topic not assigned**
- ▷ Paper: Hameed, A., Khoshkbarforoushha, A., Ranjan, R., Jayaraman, P. P., Kolodziej, J., Balaji, P., . . . & Khan, S. U. (2016). A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems. Computing, 98(7), 751-774.
  Download paper
  Abstract: *In a cloud computing paradigm, energy efficient allocation of different virtualized ICT resources (servers, storage disks, and networks, and the like) is a complex problem due to the presence of heterogeneous application (e.g., content delivery networks, MapReduce, web applications, and the like) workloads having contentious allocation requirements in terms of ICT resource capacities (e.g., network bandwidth, processing speed, response time, etc.). Several recent papers have tried to address the issue of improving energy efficiency in allocating cloud resources to applications with varying degree of success. However, to the best of our knowledge there is no published literature on this subject that clearly articulates the research problem and provides research taxonomy for succinct classification of existing techniques. Hence, the main aim of this paper is to identify open challenges associated with energy efficient resource allocation. In this regard, the study, first, outlines the problem and existing hardware and software-based techniques available for this purpose. Furthermore, available techniques already presented in the literature are summarized based on the energy-efficient research dimension taxonomy. The advantages and disadvantages of the existing techniques are comprehensively analyzed against the proposed research dimension taxonomy namely: resource adaption policy, objective function, allocation method, allocation operation, and interoperability*

10.14. **Dynamic Remote Data Auditing**

- ☒ **Presented by: Florian Berger**
- ▷ Paper: Sookhak, M., Gani, A., Khan, M. K., & Buyya, R. (2017). Dynamic remote data auditing for securing big data storage in cloud computing. Information Sciences, 380, 101-116.
  Download paper
  Abstract: *Cloud computing has emerged as a new computing paradigm that offers great potential for storing data remotely. Presently, many organizations have reduced the burden of local data storage and maintenance by outsourcing data storage to the cloud. However, integrity and security of the outsourced data continues to be a matter of major concern for data owners due to the lack of control and physical possession over the data. To deal with this problem, researchers have proposed remote data auditing (RDA) techniques. However, the majority of existing RDA techniques is only applicable for static archived data and is not applicable for auditing or dynamically updating the outsourced data. They are also not applicable to big data storage because of the high computational overhead on the auditor. In this paper, we propose an efficient RDA technique based on algebraic signature properties for a cloud storage system that incurs minimum computational and communication costs. We also present the design of a new data structure-Divide and Conquer Table (DCT)—that can efficiently support dynamic data operations such as append, insert, modify, and delete. Our proposed data structure can be applied for large-scale data storage and will incur minimum computational cost. A com- parison between our proposed method and other state-of-the-art RDA techniques shows that our method is secure and highly efficient in reducing the computational and communication costs on the server and the auditor.*

10.15. **Truthful Online Auctions**

- □ **Topic not assigned**
- ▷ Paper: Zhang, H., Jiang, H., Li, B., Liu, F., Vasilakos, A. V., & Liu, J. (2016). A framework for truthful online auctions in cloud computing with heterogeneous user demands. IEEE Transactions on Computers, 65(3), 805-818.
  Download paper
  Abstract: *Auction-style pricing policies can effectively reflect the underlying trends in demand and supply for the cloud resources, and thereby attracted a research interest recently. In particular, a desirable cloud auction design should be (1) online to timely reflect the fluctuation of supply-demand relations, (2) expressive to support the heterogeneous user demands, and (3) truthful to discourage users from cheating behaviors. Meeting these requirements simultaneously is non-trivial, and most existing auction mechanism designs do not directly apply. To meet these goals, this paper conducts the first work on a framework*

for truthful online cloud auctions where users with heterogeneous demands could come and leave on the fly. Concretely speaking, we first design a novel bidding language, wherein users' heterogeneous requirement on their desired allocation time, application type, and even how they value among different possible allocations can be flexibly and concisely expressed. Besides, building on top of our bidding language we propose COCA, an incentive-Compatible (truthful) Online Cloud Auction mechanism. To ensure truthfulness with heterogenous and online user demand, the design of COCA is driven by a monotonic payment rule and a utility-maximizing allocation rule. Moreover, our theoretical analysis shows that the worst-case performance of COCA can be well-bounded, and our further discussion shows that COCA performs well when some other important factors in online auction design are taken into consideration. Finally, in simulations the performance of COCA is seen to be comparable to the well-known off-line Vickrey-Clarke-Groves (VCG) mechanism.

10.16. **Measuring IPv6 adoption**

- ☒ **Presented by: Adrian Magnus Graën**
- ▷ Paper: J Czyz, M Allman, J Zhang, S Iekel-Johnson, E Osterweil, M Bailey: Measuring ipv6 adoption – ACM SIGCOMM Computer Communication Review - SIGCOMM'14, Volume 44 Issue 4, October 2014, Pages 87-98.

  Download paper

  Abstract: *After several IPv4 address exhaustion milestones in the last three years, it is becoming apparent that the world is running out of IPv4 addresses, and the adoption of the next generation Internet protocol, IPv6, though nascent, is accelerating. In order to better understand this unique and disruptive transition, we explore twelve metrics using ten global-scale datasets to create the longest and broadest measurement of IPv6 adoption to date. Using this perspective, we find that adoption, relative to IPv4, varies by two orders of magnitude depending on the measure examined and that care must be taken when evaluating adoption metrics in isolation. Further, we find that regional adoption is not uniform. Finally, and perhaps most surprisingly, we find that over the last three years, the nature of IPv6 utilization-in terms of traffic, content, reliance on transition technology, and performance-has shifted dramatically from prior findings, indicating a maturing of the protocol into production mode. We believe IPv6's recent growth and this changing utilization signal a true quantum leap.*

Source

Texts can be downloaded from the ☞ Learnweb-course.

List of the 13 topics which have not been assigned yet: 10.1., 10.2., 10.3., 10.4., 10.6., 10.7., 10.8., 10.9., 10.10., 10.11., 10.12., 10.13., 10.15., Please see individual papers for a description.