ACCEPTED FROM OPEN CALL

AMCLOUD: TOWARD A SECURE AUTONOMIC MOBILE AD HOC CLOUD COMPUTING SYSTEM

DEVU MANIKANTAN SHILA, WENLONG SHEN, YU CHENG, XIAOHUA TIAN, AND XUEMIN (SHERMAN) SHEN

ABSTRACT

Cloud computing is a revolutionary paradigm to deliver computing resources, ranging from data storage/processing to software, as a service over the network, with the benefits of efficient resource utilization and improved manageability. The current popular cloud computing models encompass a cluster of expensive and dedicated machines to provide cloud computing services, incurring significant investment in capital outlay and ongoing costs. A more cost effective solution would be to exploit the capabilities of an *ad hoc cloud* which consists of a cloud of distributed and dynamically untapped local resources. The ad hoc cloud can be further classified into static and mobile clouds: an ad hoc static cloud harnesses the underutilized computing resources of general purpose machines, whereas an ad hoc mobile cloud harnesses the idle computing resources of mobile devices. However, the dynamic and distributed characteristics of ad hoc cloud introduce challenges in system management. In this article, we propose a generic em autonomic mobile cloud (AMCloud) management framework for automatic and efficient service/resource management of ad hoc cloud in both static and mobile modes. We then discuss in detail the possible security and privacy issues in ad hoc cloud computing. A general security architecture is developed to facilitate the study of prevention and defense approaches toward a secure autonomic cloud system. This article is expected to be useful for exploring future research activities to achieve an autonomic and secure ad hoc cloud computing system.

INTRODUCTION

Cloud computing is a novel technology to deliver computing resources, ranging from data storage and processing to software, as a service over the network, typically using Internet technologies. The US National Institute of Standards and Technology (NIST) has categorized cloud computing into three service models [1]: software as a service, platform as a service, and infrastructure as a service. Still evolving, this revolutionary paradigm has the potential provide several benefits, including significant cost savings through increased operating and economic efficiencies, improved manageability, and reduced maintenance. Furthermore, it could also significantly boost partnership, agility, and scalability, thus facilitating a truly global computing model.

Nevertheless, existing archetypical cloud computing models (public, private, or partner) encompass a cluster of expensive and dedicated machines to run those cloud computing resources, leading to significant investment in capital outlay and ongoing costs. It is further observed that the resources inside the data centers often operate at "low utilization" due to resource stranding and fragmentation. Moreover, the energy consumed by machines housed in data centers also embodies a financial burden on the organizations that operate them as well as an infrastructure burden on power utilities.

For a cost effective cloud computing mode, ad hoc cloud computing aims to leverage untapped local computing and storage resources to form an ad hoc cloud of local resources. Based on the nature of the local resources, we categorize ad hoc cloud into two modes, ad hoc static cloud and ad hoc mobile cloud. Ad hoc static cloud harnesses the underutilized computing resources of general purpose machines owned by an enterprise, organization, or normal users. Though ad hoc static cloud shares some of the characteristics of the grid and volunteer computing, it incorporates new features, i.e. supporting diverse applications, rapid elasticity, and coordinated use of computing resources for large number of users. Ad hoc mobile cloud harnesses the idle computing resources of mobile devices owned by the same or different individuals. The concept of ad hoc mobile cloud is different from classic mobile cloud models that allow offloading of mobile applications to remote resource-rich clouds. In ad hoc mobile cloud, a local pool of smart devices (e.g. smartphones, Internet of things, etc.) will be collected and aggregated to provide sufficient resources for computationally expensive cloud services. Note that ad hoc mobile cloud is closely related to the concept of opportunistic computing, where a device can opportunistically leverage other available resources within the network. Nevertheless, ad hoc mobile cloud targets a more organized, large-scale resource sharing system through resource virtualization and system management.

Deve Manikantan Shila is with United Technologies Research Center.

Wenlong Shen and Yu Cheng are with Illinois Institute of Technology.

Xiaohua Tian is with Shanghai Jiaotong University.

Xuemin (Sherman) Shen is with University of Waterloo.

Digital Object Identifier: 10.1109/MWC.2016.1500119RP

Ad hoc cloud is expected to provision a wide range of multimedia services and applications such as distributed environment monitoring, object localization and tracking, multimedia content sharing, and ad hoc multi-party gaming. As applications are diverse in terms of scale and complexity, management of ad hoc cloud will be a costly and challenging issue due to the dynamics of resource availability and heterogeneous QoS requirements. Autonomic management, encompassing the characteristics of self-configuration, self-optimization, self-healing, and self-protection, is a promising solution for managing the ad hoc cloud computing system. Currently, the existing literature does not contain many studies on autonomic management for cloud computing. In [2], an autonomic framework, named CometCloud, is proposed to enable application workflows with diverse and changing requirements over highly heterogeneous, dynamically federated, computing and data platforms. However, CometCloud mainly considers server-oriented cloud systems, and lacks details on how to achieve autonomic management. There is emerging interest in autonomic provisioning of big data on clouds [3], where the focus is on adaptive provisioning of cloud resources to make cloud-hosted big data applications operate more efficiently rather than on the design of the autonomic management framework.

In [4], an autonomic service management framework based on coordinated integration of service-oriented architecture (SOA), application-oriented networking (AON), and autonomic computing is proposed. This framework provides automated management of network resources through optional and manageability interfaces, enabling the network designer to impose protocols and policies for different network management requirements. In this article, we propose, based on [4], to establish an autonomic mobile cloud (AMCloud) management system for ad hoc cloud computing. The most related work to AMCloud is [5], which proposes an autonomic resource provisioning framework for organizing the heterogeneous sensing, computing, and communication capabilities of static and mobile devices in the vicinity to form an elastic resource pool. Nevertheless, the main contribution of [5] is in the area of adaptive energy-aware and uncertainty-aware resource allocation engines; a systematic design of the autonomic management framework for ad hoc cloud is still not available.

Though envisioned to improve investment and energy savings, utilization, and lifetime, ad hoc cloud computing lacks sufficient security and privacy guarantees due to its distributed architecture and dynamic environment [6]. While there are some studies on the security of mobile cloud computing, few examine the ad hoc mobile cloud computing model. The work in [7] discusses the security issues in the context of a general ad hoc network, but does not clearly address the issues unique to ad hoc cloud computing. Furthermore, none of the existing autonomic studies mentioned above and the references therein incorporate security issues into the system.

This article provides an overview of the ad hoc cloud architecture, addresses the network/service management issue, analyzes potential security and privacy threats, and presents attack countermeasures and research challenges, with the objective of developing solutions toward a secure autonomic mobile cloud system. This article should be useful for exploring future research activities to achieve an autonomic and secure ad hoc cloud computing system.

Ad Hoc Cloud Computing

This section first reviews existing ad hoc cloud architecture designs, and then proposes an autonomic mobile cloud (AMCloud) management framework.

Ad Hoc Static Cloud Computing

A large amount of computational and storage resources within organizations, enterprises, and homes are often under exploited. Leveraging these untapped resources for cloud computing services instead of dedicated data center machines will yield various benefits. First, it could amortize the number of commodity servers, backups, storage, switches, and other IT equipment that needs to be procured. Second, it could lead to better utilization of idle resources. Finally, it could reduce overall power usage and costs. If we rely on non-dedicated machines housed in working spaces for computing resources, and given that they are placed at lower densities compared to data centers, the energy consumed for power conditioning, heating, and cooling can be controlled easier.

A cloudlet based architecture for an ad hoc static cloud computing model is proposed in [8]. The purpose of cloudlet is to render particular services or applications that can be accessed by participating nodes through web services or other suitable protocols. In the cloudlet based architecture, each node runs software called a cloud element, which encompasses two main components: an engine capable of running the workloads associated with its cloudlet functionality; and a modeler/manager that has knowledge of the semantics of the workload and a cost model that enables analysis about how the workloads will be executed. Note that the purpose of the modeler/manager is to control the operation of its associated engine for optimal performance and to distribute information to support effectual placement and adaptation of cloud elements. In addition to cloud elements, each node also employs cloud infrastructure software that supports the creation, management, and destruction of cloud elements. In particular, the cloud infrastructure contains an element manager for creating and destroying cloud elements; an infrastructure modeler/manager that interacts with the host operating system to monitor the effects of the local cloud elements on user processes, and vice versa; and a broker and dispatcher for quality of service(QoS) provisioning.

Ad Hoc Mobile Cloud Computing

A handful of research efforts have been conducted on mobile cloud computing that enables offloading of mobile applications to remote clouds and the provisioning of services from resource-rich cloud to mobile devices. Ahile the offloading paradigms resolve some important issues in mobile computing, such as resource sparseness,

A large amount of computational and storage resources within organizations, enterprises, and homes are often under exploited. Leveraging these untapped resources for cloud computing services instead of dedicated data center machines will enable various benefits.

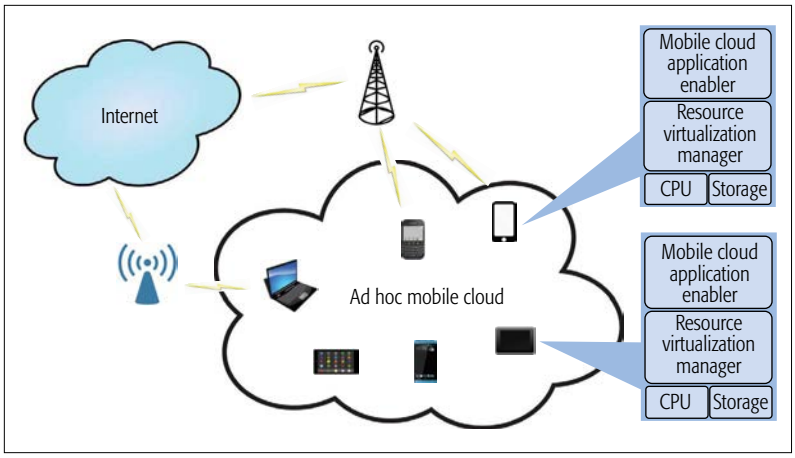

Figure 1. Mobile ad hoc cloud architecture.

hazardousness, and limited energy sources, success depends on the connection to the remote cloud, and it has been seen that such approaches often fail in scenarios where the connection to a remote cloud is not always available. The ad hoc mobile cloud takes a different paradigm to exploit the available computing resources within the mobile devices ad hoc networked to realize a common goal in a distributed fashion. A typical ad hoc mobile cloud model is illustrated in Fig. 1. Most of the local cloud resources will be mobile devices owned by different individuals, such as laptops, tablets, and smartphones. Each mobile device normally needs to incorporate a "resource virtualization manager" that enables the sharing of resources within the mobile among different cloud applications, and a "mobile cloud application enabler" that enables connection among the mobile devices to form an ad hoc cloud. More details regarding the ad hoc cloud architecture are to be presented in the AMCloud framework.

Ad hoc cloud computing is envisioned to offer several benefits, such as the availability of local cloud services and better utilization of unexploited resources. In particular, smartphones are turning into the "do it all" device, replacing laptops and PCs for many traditional applications such as email, web surfing, and e-commerce. A local ad hoc mobile cloud formed out of smartphones has the potential to offer sufficient resources for computationally expensive cloud services. In addition, smartphones have a variety of sensing abilities that can also be used to render context-aware services for users. Recently, with the "bring your own device" (BYOD) paradigm, enterprise IT departments have started allowing employees to perform work related tasks on their personal phones.

A framework for ad hoc mobile cloud computing is proposed in [9], consisting of the following three components.

- A **resource handler** is responsible for the discovery of potential clients within a neighborhood, establishing connections and exchanging device data such as processor type, battery life, and processing pricing. The context manager and resource monitor within the resource handler are responsible for sensing, recording contextual information about clients (e.g. location, velocity, mobility), and keeping track of clients.
- A **cost handler** is responsible for estimating costs and selecting suitable client devices based on device data, user priorities, requirements, and constraints. A micropayment module is included to support the payment transactions between the client devices and owner device.
- A **job handler** is responsible for dynamically partitioning the application based on the resources and capabilities of each potential client device, creating job pools and the handling job distribution and scheduling mechanism. However, the framework does not incorporate security management mechanisms.

Autonomic Mobile Cloud Management Framework

Due to the dynamic and distributed characteristics of ad hoc cloud computing networks, the management of such a system has become one of the most challenging issues. Enlightened by the autonomic service management framework in reference [4], here we propose an autonomic mobile cloud (AMCloud) management framework, for automatic, scalable, and efficient service/resource management over the ad hoc cloud computing network. Note that the AMCloud architecture stands for a general management framework for ad hoc cloud computing in both the static and mobile modes; the static mode can be considered as a simplified case of the mobile mode.

The proposed AMCloud management framework is shown in Fig. 2, where cloud applications are created and managed by a mobile cloud application-enabling fabric (MCAEF) as a composition of manageable autonomic cloud elements. Each autonomic cloud element basically virtualizes physical resources according to the "monitor, analyze, plan, and execute" autonomic control loop; an autonomic cloud element could also be provisioned by combining other cloud elements. Each autonomic cloud element is wrapped with a common interface to facilitate communications among them.

One key feature of the autonomic cloud element is the automated management of virtualized resources through optional and manageability interfaces, with supporting knowledge of the computing environment and management policies. The separation of optional interface and manageability interface is intended to facilitate business application composition and management application composition, respectively. Both types of interfaces can be simultaneously involved in a cloud service composition process. Considering autonomic cloud computing requirements, we enhance the manageability interfaces defined in [4] into interfaces for semantic description, SLA negotiation, autonomic manager (sensor and effector), and security. The semantic description interface aims at adding machine-interpretable information to the autonomic cloud element optional interface to enable automatic cloud service discovery and composition. The SLA (service-level agreement) negotiation interface executes the SLA negotiation procedure, which defines the cloud service performance metrics, QoS levels, as well as accounting related rules, and the lifecycle of the cloud service. The autonomic manager (sensor and

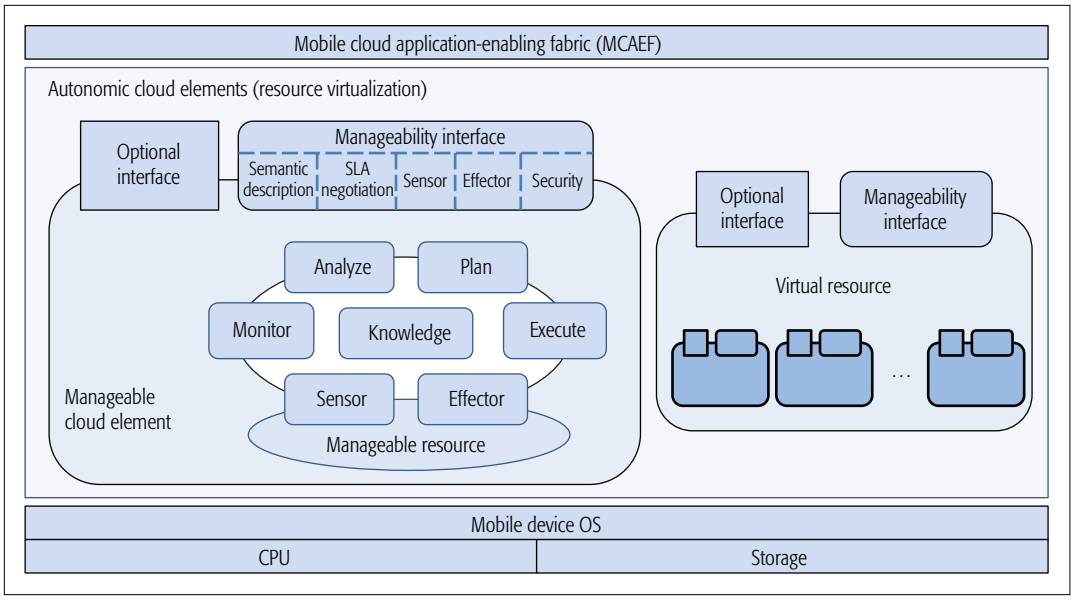

Figure 2. Autonomic Mobile Cloud (AMCloud) management framework.

effector) interfaces enable autonomic management of the cloud element, including obtaining data from the manageable resource and performing operations on the manageable resource. The security interface imposes security protocols on the cloud service, protecting the integrity and confidentiality of data in cloud services.

There is still much work to be done to develop an autonomic mobile cloud management framework, requiring much research work to determine the implementation details for each interface. The rest of this article will focus on the security interface design.

Potential Security and Privacy Challenges

In mobile ad hoc cloud, security is an indispensable component involved in various functions such as discovery of devices, partitioning of workload, processing of tasks outsourced from other devices, communicating the results among devices, and incentive mechanisms. These functions can be easily jeopardized if countermeasures are not embedded into the ad hoc cloud computing model at the early stages of design. Although establishing a priori trust may solve most of the security concerns, it is not practically feasible in mobile ad hoc cloud due to the dynamicity and anonymity of devices involved in the communication, which makes the key management and entity authentication schemes hard to realize. In the following sections, we analyze some important attacks associated with mobile ad hoc cloud computing according to three categories: cloud application attack, protocol attack, and device attack.

Cloud Application Attack

Selfish Attack: Most of the existing studies in the area of ad hoc cloud computing assume that devices are always willing to participate. The assumption of cooperativeness may be reasonable in some settings but not generally valid. For example, processing data for other devices may blow up the battery of the device. A general and practical mobile ad hoc cloud framework needs to consider selfish devices (or devices launching selfish attacks) that aim to:

- Increase their revenue by accepting larger payments for processing tasks for other devices.
- Increase battery lifetime by driving fellow devices to execute its tasks at a lower cost or refusing to process tasks for others.

Further, there could exist cheating devices that accept payment and later on play dead by simply refusing to process tasks for others.

Workload Distribution Attack: By manipulating the workload or tasks distributed to mobile nodes, an attacker can launch a variety of attacks. For example, an attacker can purposely partition computationally intensive tasks (but without meaningful application purposes) among the legitimate devices to drain its energy and cause a denial of service attack. Another issue is how to isolate highly sensitive information from other non-sensitive information. There should be a clear distinction of how the tasks are split among the devices so that highly sensitive information or tasks do not fall into the wrong hands. Although task distribution normally incorporates privacy protection mechanisms so that individual devices would not obtain knowledge of the actual mission of the original task, an attacker might compromise several devices and these devices can collude to construct the entire original task.

Communication Infrastructure Attack

Communication Link Attack: Ad hoc cloud normally involves networking communications between local resources via wired (Ethernet) or wireless (Wi-Fi, Bluetooth, NFC) connections. If not properly secured, these digital connections are vulnerable to a variety of attacks that challenge the three basic principles of security: confidentiality, integrity, and availability. Some common attack vectors include eavesdropping, fabrication, tampering, and denial of service attacks. For instance, by surreptitiously listening to communication between the local resources,

In mobile ad hoc cloud, security is an indispensable component involved in various functions such as discovery of devices, partitioning of workload, processing of tasks outsourced from other devices, communicating the results among devices, and incentive mechanisms.

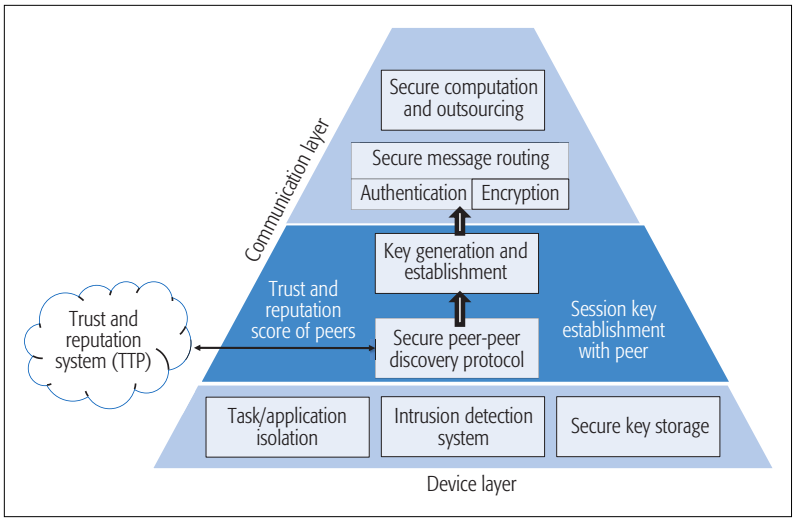

Figure 3. Proposed security architecture.

an attacker can gain critical information pertaining to services and payment transactions, and thereby their whereabouts. With enough messages collected, the attacker may extract knowledge about the user and location profiles, and later use this knowledge to launch some potential burglary action. Another concern is the relay attack, where the attacker captures the payment information of other devices to pay for its cost of service at a later point in time.

Cloud Availability Attack: Provisioning ad hoc cloud services normally involves three stages [8, 9]: discovery of potential devices based on available resources and pricing; partitioning of tasks; and processing of tasks and communicating the results back. Attacks at stage 1 and stage 2 may severely impact the availability of the cloud services. *Discovery attack*: A typical threat model is that the attackers respond with misleading messages (e.g. availability of computational resources, better pricing models) and thus create a large circle of influence by attracting traffic from legitimate nodes. An adversary could also broadcast bogus task requests to legitimate nodes to launch a flooding attack. *Processing and communicating attack*: A typical threat model will be when an adversary lures tasks into itself through discovery attacks and then computes erroneous information or communicates false results back to the originator. Attackers may also act dead by not responding back.

Device Attack

A security issue particularly for mobile ad hoc cloud is that mobile devices have limited computing resources or power to run advanced intrusion detection systems, so it will be easier (compared to cloud over PCs or servers) for an attacker to gain control of the device through the installation of malware embedded in a task. Upon installation, the malware can do several attacks:

- Accesses sensitive information residing in the devices (e.g. cryptographic information, social networking information) and transfer it to the attacker (e.g. *Loozfon*, an information-stealing malware, and *FinFisher*, a spyware capable of taking over a mobile device.)
- Compromises the device by unlocking the secure locked boot loaders. The devices are particularly vulnerable during the power-up sequence, and unlocked boot loaders can be used either to interrupt the power-up (boot-up) sequences (a denial of service attack) or run a program different from the intended program to compromise the device.
- Escalates the access privilege by disabling certain restrictions imposed by the device manufacturer or cell phone carrier through jail breaking or rooting. This enables the attacker nearly unregulated control over which programs can be installed and how the device can be used.
- Accesses other users' data and information.

Security Architecture for Ad Hoc Cloud Computing

According to the security challenges discussed above, we investigate the possible defense solutions against those attacks, as well as the research challenges and gaps associated with these solutions. We then propose a general security architecture for ad hoc cloud computing.

Attack Prevention and Defense

Reward and Reputation System: Offering cooperative ad hoc cloud users certain types of "rewards" is a promising solution to deal with the selfish issue in an ad hoc cloud environment. The reward system can be based on reputation value or virtual credit: cooperative users earn reputation and virtual credits; users pay virtual credits to publish a cloud task. The discovery attack, workload division attack, and processing and communicating attack are also possibly solved by a proper reward system: attackers responding with misleading messages will have a low reputation; posting tasks to cause a denial of service attack will cost the attacker a large amount of virtual credits; luring the traffic but not fulfilling the cloud task will result in a reputation punishment. When the reputation value or virtual credits of a node drops below the threshold, it will be denied to participate the ad hoc cloud network. Many existing research works have developed different kinds of reward systems for ad hoc network routing behavior [11], and the incentives for cooperation in these reward systems have been studied from the perspective of game theory analysis [10]. However, research attention still needs to adapt these reward systems to an ad hoc cloud computing environment, as well as deal with problems such as malicious nodes falsifying their reputation values.

Secure the Communication Infrastructures: To protect the confidentiality, integrity, and availability of cloud data while being transmitted, proper encryption algorithms as well as secure routing protocols are necessary. Encryption algorithms protect cloud data from attacks such as eavesdropping and modification, while secure routing protocols guarantee data availability. Secure routing protocols for ad hoc networks have been extensively studied, and these routing protocols are ready to be applied in ad hoc cloud computing. However, designing a cryptographic scheme for ad hoc cloud users presents a non-trivial issue. The lack of pre-shared secrets

among users and the absence of public key infrastructure in ad hoc network environments make it very difficult to generate reliable cryptographic keys. One possible solution is to have all ad hoc cloud users install software that serves as a trusted authority or public key infrastructure. However, maintaining such software will introduce extra management overhead.

Malware Detection and Task Isolation: The attacks of intrusion and privilege violation and nefarious use of computing have one common feature: the attackers try to embed malicious codes into their cloud tasks and have them run on other users' devices. To prevent this, two layers of protection are needed: a cloud task isolation mechanism, and a malware detection system (anti-virus software). Cloud task isolation is an important research issue in cloud computing, and some efforts have been made in the literature such as [12]. However, migrating those defense mechanisms to mobile device operating systems still needs research efforts. Some malware detection systems for mobile devices have already appeared on the market, but further studies are required to improve the capability and efficiency of those detection systems.

Secure Interface Architecture for AMCloud Framework

Based on the discussions and analysis presented above, the security objectives for a trustable ad hoc cloud computing network can be summarized as follows. Cloud users have incentives to participate in cloud tasks; the confidentiality, integrity, and availability of cloud data can be guaranteed; privacy information of cloud users is well protected; user devices in the cloud are free from malware infection. Having these goals in mind, we design a secure interface architecture for the aforementioned AMCloud management framework, as shown in Fig. 3.

The proposed security interface architecture consists of several security components, and these components further form into two layers of protection: the device layer protection and the communications layer protection.

Device Layer Protection: There are three security components in the device layer: task/application isolation, intrusion detection system, and secure key storage. These three components keep users' local privacy data from leaking to the cloud, as well as prevent malicious malware from damaging cloud users' devices. Task/application isolation forms a "boundary" between cloud tasks and local data or processes while they are sharing the same physical device, restricting the computation and memory resources that a cloud task occupies. The intrusion detection system may detect malicious codes injected into the incoming cloud tasks, and warn the user when their private data are leaking to the cloud. Secure key storage will impose an extra layer of protection for crucial sensitive data such as encryption keys, account passwords, and financial related information, minimizing the risk of leakage of this information.

Communication Layer Protection: Communication layer protection starts the moment a user joins an ad hoc cloud. A secure peer-peer discovery protocol helps cloud users wisely chose their cloud task participants by eliminating malicious or misbehaving users based on information from the trust and reputation system; such information includes nodes' reputation value, behavior history, available resources, and pricing, as well as social network related information. After the peer discovery phase, a session key for the cloud task should be established among all cloud task participants through key generation and establishment. This established session key will be used to encrypt the cloud data, protecting the confidentiality and integrity while the cloud data is being transmitted via the wireless channel. The relay of cloud data follows the secure message routing protocols, thus guaranteed to be delivered to the desired user. In addition, the secure computation and outsourcing component validates the cloud computing results, at the same time protecting the privacy of the outsourced data.

Research Motivated by AMCloud

The proposed AMCloud framework is expected to facilitate future research activities toward an autonomic and secure ad hoc cloud computing system. We now discuss three threads of important research motivated by AMCloud.

Developing Secure Distributed Computing Algorithms

To fully exploit the benefits of ad hoc cloud, an application needs to be equipped with the capability to be decomposed into multiple tasks, which can be executed by different AMcloud elements in a distributed manner. While developing secure distributed algorithms for parallel computing is of fundamental importance to ad hoc cloud, it is still a widely open research area and most of the existing studies just assume that task parallelism is available [5]. Driven by the AMCloud and motivated by the open issue of task parallelism, we conducted some pioneering work on developing a distributed secure outsourcing scheme for solving linear algebraic equations (LAE) in ad hoc cloud [13]. The original LAE problem is decomposed into subproblems; all involved agents then apply a consensus based algorithm to obtain the correct solution in a distributed and iterative manner. We further identify a number of security risks in this process, and propose a secure outsourcing scheme that can preserve privacy to shield the original LAE parameters and the final solution from the computing agents, and also detect misbehavior based on mutual verifications in a real-time manner.

Adaptive Resource Allocation Techniques in Ad Hoc Mobile Cloud

An underpinning concept in cloud computing is resource virtualization. A network node can provision its physical resources to multiple applications through certain service level agreements. The significant challenge is to design proper adaptive resource allocation techniques to balance the tradeoff between resource utilization efficiency and QoS guarantees. An ad hoc mobile cloud embraces inherent uncertainty in terms of network connectivity and device availability,

An underpinning concept in cloud computing is resource virtualization. A network node can provision its physical resources to multiple applications through certain service level agreements. The significant challenge is to design proper adaptive resource allocation techniques for balancing the tradeoff between resource utilization efficiency and QoS guarantee.

The ad hoc cloud computing paradigm is envisioned to reduce cost and improve energy efficient, compared to data-center based cloud computing model, through exploiting distributed and dynamic untapped local resources. Nonetheless, the distributed and dynamic characteristics of the paradigm present extra management difficulty and security concerns.

attributed to unstable communication channel quality, high node mobility, complex co-channel interference, heterogeneous rate of energy drain, and other factors. Furthermore, traffic load and QoS requirements from a service requester can also change dynamically. With AMCloud, adaptive resource allocation requires cooperation at both the cloud element level and the MCAEF level. At the element level, the autonomic control loop needs to achieve a proper context-aware resource allocation engine for QoS provisioning even under uncertainties. For example, the study in [14] proposes an online video frame selection algorithm for mobile cloud gaming to minimize the total distortion based on the network status, input video data, and delay constraint. At the MCAEF level, the cloud application enabling fabric needs to coordinate multiple related elements to provision the end-to-end QoS guarantee. Some important issues such as routing, cluster formation, and service query and composition all need to be addressed at the MCAEF level; the solution should also be able to adapt to context dynamics.

Security Protocols for Smartphone-to-Smartphone Networking

Referring to the proposed security architecture, we can examine and better understand the security performance of the existing smartphones if they are involved in ad hoc mobile cloud computing. While there are existing studies on the device layer security solutions for smartphones, security solutions for communication layer protection in an ad hoc cloud context is basically an open area. The Wi-Fi direct standard has recently been developed for smartphone to smartphone communications, which enables the networking infrastructure for an ad hoc mobile cloud. However, security solutions over Wi-Fi direct [15], such as secure peer discovery, key establishment, reputation systems, and secure routing, are all open issues. In a scenario with high mobility, the established secure keys further need to be dynamically updated, due to time-variant network topology, with mobile users joining or leaving the network and the possibility that certain mobile nodes may be compromised or captured. Thus, a proper key management scheme with the capability of key updating and revocation is of critical importance for providing both forward security (i.e. preventing a leaving node from decrypting future messages) and backward security (i.e. keeping history records confidential from a newly joining mobile node). The general AMCloud framework and the security interface architecture proposed in this article are expected to guide researchers to study related security problems in a systematic manner.

Conclusions

The ad hoc cloud computing paradigm is envisioned to reduce cost and improve energy efficiency, compared to the data-center based cloud computing model, through exploiting distributed and dynamic untapped local resources. Nonetheless, the distributed and dynamic characteristics of the paradigm present extra management difficulty and security concerns. In this article, we have reviewed existing ad hoc cloud architecture designs, and further presented the autonomic mobile cloud management framework. We have also thoroughly investigated the security and privacy challenges associated with the ad hoc cloud computing model, and developed a general security architecture to facilitate the study of preventive and defense approaches toward a secure mobile cloud computing system. This article should shed some light on the directions for future research activities toward the achievement of the autonomic and secure mobile cloud system.

Acknowledgment

This work was supported in part by the NSF under grants CNS-1320736 and ECCS-1610874.

References

[1] L. M. Vaquero *et al.*, "A Break in the Clouds: Towards a Cloud Definition," *Proc. ACM SIGCOMM Computer Commun. Review*, vol. 39, no. 1, 2008, pp. 50–55.
[2] J. Diaz-Montes *et al.*, "CometCloud: Enabling Software-Defined Federations for End-to-End Application Workflows," *IEEE Internet Comp.*, vol. 19, no. 1, 2015, pp. 69–73.
[3] R. Ranian *et al.*, "Recent Advances in Autonomic Provisioning of Big Data Applications on Clouds," *IEEE Trans. Cloud Comp.*, vol. 3, no. 2, Apr./June 2015, pp. 101–04.
[4] Y. Cheng, A. Leon-Garcia, and I. Foster, "Towards an Autonomic Service Management Framework: A Holistic Vision of SOA, AON, and Autonomic Computing," *IEEE Commun. Mag.*, vol. 46, no. 5, pp. 138–46, May 2008.
[5] H. Viswanathan *et al.*, "Uncertainty-Aware Autonomic Resource Provisioning for Mobile Cloud Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 8, Aug. 2015, pp. 2363–72.
[6] L. Wei *et al.*, "Security and Privacy for Storage and Computation in Cloud Computing," *Information Sciences*, 258, 2014, pp. 371–86.
[7] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, 1999, pp. 24–30.
[8] G. Kirby *et al.*, "An Approach to Ad Hoc Cloud Computing," arXiv preprint arXiv: 1002.4378, 2010.
[9] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile Cloud Computing: A Survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84–106, 2013.
[10] Z. Li and H. Shen, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Comp.*, vol. 11, no. 8, 2012, pp. 1287–303.
[11] M. T. Refaei *et al.*, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," *IEEE Trans. Comp.*, vol. 59, no. 5, May 2010.
[12] F. Hao *et al.*, "Secure Cloud Computing with a Virtualized Network Infrastructure," *Proc. 2nd USENIX Conf. Hot Topics in Cloud Computing*, 2010.
[13] W. Shen *et al.*, "A Distributed Secure Outsourcing Scheme for Solving Linear Algebraic Equations in Ad Hoc Clouds," arXiv preprint arXiv: 1504.01042, 2015.
[14] J. Wu *et al.*, "Enabling Adaptive High-Frame-Rate Video Streaming in Mobile Cloud Gaming Applications," *IEEE Trans. Circuits Syst. Video Tech.*, vol. 25, no. 12, Dec. 2015, pp. 1988–2001.
[15] W. Shen *et al.*, "Secure Key Establishment for Device-to-Device Communications," *Proc. IEEE GLOBECOM*, pp. 336–40, 2014.

Biographies

Devu Manikantan Shila (manikad@utrc.utc.com) received her M.S. and Ph.D. degrees, both in computer engineering from the Electrical and Computer Engineering Department at Illinois Institute of Technology, Chicago, USA, in 2007 and 2011, respectively. She is now working with the United Technologies Research Center as a principal investigator and project leader in the cyber physical security domain. Her research interests include wireless networking, software defined radios, cloud computing, enbedded systems, and cyber security.

WENLONG SHEN (wshen7@hawk.iit.edu) received his B.E. degree in electrical engineering from Beihang University, Beijing, China, in 2010, and the M.S. degree in telecommunication from the University of Maryland, College Park, MD, USA, in 2012. He is currently pursuing his Ph.D. degree with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. His current research interests include wireless networking, cloud computing, and network security.

YU CHENG [S'01, M'04, SM'09] (cheng@iit.edu) received B.E. and M.E. degrees in electronic engineering from Tsinghua University in 1995 and 1998, respectively, and a Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2003. He is now an associate professor in the Department of Electrical and Computer Engineering, Illinois Institute of Technology. His research interests include wireless network performance analysis, network security, and next-generation Internet technology. He received a Best Paper Award at QShine 2007, IEEE ICC 2011, and a Runner-Up Best Paper Award at ACM MobiHoc 2014. He received the National Science Foundation (NSF) CAREER Award in 2011 and an IIT Sigma Xi Research Award in the junior faculty division in 2013. He has served as a Symposium Co-Chair for IEEE ICC and IEEE GLOBECOM, and Technical Program Committee (TPC) CoChair for WASA 2011 and ICNC 2015. He is a founding Vice Chair of the IEEE ComSoc Technical Subcommittee on Green Communications and Computing. He is an associate editor for *IEEE Transactions on Vehicular Technology*, and the editor of the New Books & Multimedia Column for *IEEE Network*.

XIAOHUA TIAN [S'07, M'11] (xtian@sjtu.edu.cn) received his B.E. and M.E. degrees in communication engineering from Northwestern Polytechnical University, Xi'an, China, in 2003 and 2006, respectively. He received the Ph.D. degree from the Department of Electrical and Computer Engineering (ECE), Illinois Institute of Technology (IIT), Chicago, in Dec. 2010. Since Mar. 2011 he has been with the School of Electronic Information and Electrical Engineering at Shanghai Jiao Tong University, and now is an associate professor.

XUEMIN (SHERMAN) SHEN [M'97, SM'02, F'09] (sshen@uwaterloo.ca) is a professor and university research chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is also the associate chair for graduate studies. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He is an elected member of the IEEE ComSoc Board of Governor, and the chair of the Distinguished Lecturers Selection Committee. He has served as the Technical Program Committee chair/co-chair for IEEE Globecom'16, Infocom'14, IEEE VTC'10 Fall, and Globecom'07. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo. He is a registered professional engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and the IEEE Communications Society.