A COMPREHENSIVE ANALYSIS OF PREVENTING ATTACKS OVER VIRTUAL CLOUDS

C.Swathi[1], R.Kalavathi[2], A.Yashwanth Reddy[3]
[1,2,3] Assistant Professor, Sree Dattha Group of Institutions, Hyderabad, Telangana,

Abstract

SDN-based core network is introduced in the GCN architecture by replacing the traditional Evolved Packet Core in the LTE network in order to provide efficient communications connections between different end points. The Cloudlet Network File System (CNFS) is designed based on the proposed architecture in order to protect the Avatars' dataset against hardware failures and improve Avatars' performance in terms of data access latency. Moreover, a green energy supplement is proposed in the architecture in order to reduce the extra OPEX footprint incurred by running the distributed cloudlets. Due to the temporal and spatial dynamics of both the green energy generation and energy demands of green cloudlet systems (GCSs), designing an optimal green energy management strategy based on the characteristics of green energy generation and the energy demands of eNBs and cloudlets to minimize the on-grid energy consumption is critical to the cloudlet provider. It presents a new cloudlet net architecture for security enforcement to establish trusted mobile cloud computing. The cloudlet net is Wi-Fi- or mobile-connected to the Internet. This security framework establishes a cyber reliance shield to fight against intrusions to distance clouds, prevent malicious attacks on mobile cloud resources, and stop unauthorized access of shared datasets in offloading the cloud.

Keywords: Cloudlet net, inter-cloud protocol, collaborative intrusion detection, cloud mashup.

1. INTRODUCTION

Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. The ultimate goal of MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience. MCC provides business opportunities for mobile network operators as well as cloud providers. More comprehensively, MCC can be defined as "a rich mobile computing technology that leverages unified elastic resources of varied clouds [1] and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle." Mobile cloud computing becomes an emerging field with high hope by massive users. We aim to support mobile devices (smartphones, tablets. Etc.) to access cloud services via WiFi or mobile grids. Cloudlets have been proposed as wireless gateways to access remote clouds. Cloudlets and WiFi access points (wireless routers) are integrated to form WiFi-enabled cloudlets. MCC uses computational augmentation approaches (computations are executed remotely instead of on the device) by which resource-constraint mobile devices can utilize computational resources of varied cloud-based resources. In MCC, there are four types of cloud-based resources, namely distant immobile clouds, proximate immobile computing entities, proximate mobile computing entities, and hybrid (combination of the other three model). Giant clouds such as Amazon [2] EC2 are in the distant immobile groups whereas cloudlet or surrogates are member of proximate immobile computing entities. Smartphones, tablets, handheld devices, and wearable computing devices are part of the third group of cloud-based resources which is proximate mobile computing entities.

Although significant research and development in MCC is available in the literature, efforts in the following domains are still lacking:

Architectural issues: A reference architecture for heterogeneous MCC environment is a crucial requirement for unleashing the power of mobile computing towards unrestricted ubiquitous computing.

Energy-efficient transmission: MCC requires frequent transmissions between cloud platform and mobile devices, due to the stochastic nature of wireless networks, the transmission protocol should be carefully designed.

Context-awareness issues: Context-aware and socially-aware computing are inseparable traits of contemporary handheld computers [3-6]. To achieve the vision of mobile computing among heterogeneous converged networks and computing devices, designing resource-efficient environment-aware applications is an essential need.

Live VM migration issues: Executing resource-intensive mobile application via Virtual Machine (VM) migration-based application offloading involves encapsulation of application in VM instance and migrating it to the cloud, which is a challenging task due to additional overhead of deploying and managing VM on mobile devices.

Mobile communication congestion issues: Mobile data traffic is tremendously hiking by ever increasing mobile user demands for exploiting cloud resources which impact on mobile network operators and demand future efforts to enable smooth communication between mobile and cloud endpoints.

Trust, security, and privacy issues: Trust is an essential factor for the success of the burgeoning MCC paradigm. It is because the data along with code, component, application, complete VM is offloaded to the cloud for execution. Moreover, just like software and mobile application piracy, the MCC application development models are also affected by the piracy issue. Pirax is known to be the first specialized framework for controlling application piracy in MCC environment. Mobile devices submit their cloud access requests through the cloudlet net.

Mobile cloud computing uses cloud computing to deliver applications to mobile devices. These mobile apps can be deployed remotely using Speed and flexibility and development tools. On the cloMobile cloud applications can be built or revised quickly using cloud services. They can be delivered to many different devices with different operating systems. Thus, users can access applications that could not otherwise be supported. Our cloud-based security system works as an intelligent firewall or intrusion detection system (IDS) to secure mobile devices within the range of the underlying WiFi net. This approach extends from previous approaches. We aim to improve in the following aspects:

(1) We propose a hierarchically designed security constructed. A trust chain is established between mobile devices, the cloudlet net, and remote cloud platforms.

(2) Predictive security analytics are processed at the backend cloud for virus signature scanning and update with automated malicious filtering and removal.

(3) We emphasize real-time filtering or removal of malicious attacks or fast response to intrusions with the help of trusted remote clouds.

2. EXISTING STRATEGIES

R. Reeder and S. Schechter work on secondary verification, accent the preponderant problem of assembling a supply of tool that can be trailer-made to fit each user’s security and reliability needs. The security of these questions has received limited formal scan, almost all of which pace smart-phone.

Stuart Schechter and Cormack Harley deals with User-selected passwords are subject to arithmetical guessing thrust, a form of reference thrust, in which an thrust sorts the password reference by rely, or previously-observed, popularity and guesses the most popular passwords first. Password-health meters provide auspices based on rules orient to those used to erect password custom, but the hazard classic under which they give this ‘strength’ is dim. Thus, most online tenacity meters will deem a string of 32 random lowercase letters a ‘weak’ password.

Alain Mayer, Fabian Monroe, Michael K. Reiter deals with, in this papers us far advance the theory and practice of graphical passwords. We take as a main benchmark the need to gauge graphical passwords' security relative to that of extols passwords. We design two graphical password schemes that we believe to be more secure than extols passwords. Throughout this paper we focus on dotted passwords that are repeatable by the user. This divide our work from all works on dotted pattern notice of which we are aware where it success for the device to notice an input as being necessarily. Because pattern respect schemes require the storage of the plain-text password on the device, the password is vulnerable to an attacker who captures and probes the device. In contrast, because graphical passwords are retable, our schemes can derive a secret key.

Graphical input resource enable the user to duple the position of inputs from the mortal order in which those inputs occur, and we show that this duple can be used to generate password schemes with in fact larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the great passwords that, we believe, is itself a contribution. In this work we are primarily motivated by devices. Samuli Hemminki, Petteri Nurmi, Sasu Tarkoma deals with we present novel accelerator based techniques which can be used single, or in conjunction with other sensors for portage mode expose on smart phones. We focus on accelerator as they are well-suited to overcome the above mention limitations. First, accelerators have very low power consumption, enabling continuous transportation behavior monitoring. Second, accelerator measure user’s going directly and therefore do not depend on any external signal sources. Third, accelerator contains highly detailed information about phone movement, enabling fine-grained distinction of different motorized transportation modalities. Mike Just deals with this paper reports on an experimental survey into user chosen questions. We collected questions from a large mate of students, in a way that encouraged participants to give practical data.

The questions allow us to consider possible modes of attack and to judge the near effort needed to crack a question, according to a new model of the knowledge of the attacker.
Using this model, we found that many members were likely to have chosen questions with low decay answers, yet they believed that their challenge questions would stay attacks from a new arrival. Though by asking multiple questions, we are able to show a marked improvement in security for most users. In a second stage of our experiment, we applied existing advantage to measure the worth of the questions and answers. Although having youthful memories and choosing their own questions, users made errors more often than desirable.

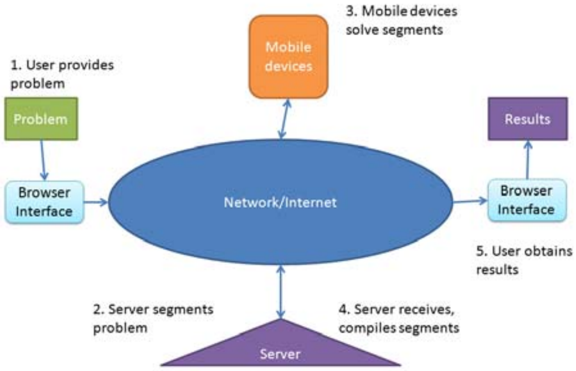

Figure 1: Proposed System Formulation

3. PROPOSED CLOUD SYSTEM

All cloudlets are Wi-Fi-enabled. Each cloudlet server has a surrounded Wi-Fi entree socket. Therefore, each cloudlet could connect too many mobile devices within the Wi-Fi range. The cloudlets are organized by whichever wired or wireless links to form the net. All cloudlets activate fundamentally as gateways at the edge network of the Internet. Remote clouds are assumed accessible through the Internet backbone.

Mobile devices are subject to malicious attacks. Encryption may not be the best solution for mobile devices due to their incomplete computing power and energy consumption limits. Some special software tools are available to resist malicious on mobile devices.., we suggest unload the data file to the cloud as most smartphone users choose to do. The remote cloud essentially provides Security as a Service to all end users. The cloud has the data-mining power to provide security intellect and investigation tools. The overall security of the mobile situation could be improved with some living cloud services such as report service, accessible storage, elastic Map Reduce in the AWS cloud. We define a new Inter-Cloudlet Protocol (ICP) for communiqué among the cloudlets in the net. This ICP protocol supports collective interruption detection and load matching operations, which are clear to mobile users. We use multiple cloudlets, each installed with an intrusion detection system (IDS). Each cloudlet has a database containing a white list of friendly users. This protocol specifies the steps needed to locked inter-cloudlet communications and load matching within the cloudlet net.

The incoming communication, if it is sufficiently small in size, will be scanned by malicious package in the getting cloudlet. However for larger file elsewhere sure limit, the sifting tasks will be offloaded to a distance cloud. Finally, when malicious is done, a notification will be returned to the bidding mobile device. Multi-party verification is applied in the cloudlet net verification which enables single sign-on within the cloudlet net.

4. CONCLUSION

The Cloudlet Network File System (CNFS) is designed based on the proposed architecture in order to protect the Avatars' dataset against hardware failures and improve Avatars' performance in terms of data access latency. Moreover, a green energy supplement is proposed in the architecture in order to reduce the extra OPEX footprint incurred by running the distributed cloudlets. Due to the temporal and spatial dynamics of both the green energy generation and energy demands of green cloudlet systems (GCSs), designing an optimal green energy management strategy based on the characteristics of green energy generation and the energy demands of eNBs and cloudlets to minimize the on-grid energy consumption is critical to the cloudlet provider. It presents a new cloudlet net architecture for security enforcement to establish trusted mobile cloud computing. The cloudlet net is Wi-Fi- or mobile-connected to the Internet.

REFERENCES

[1] Khan, A. u R.; Othman, M.; Madani, S. A.; Khan, S. U. (2014-01-01). "A Survey of Mobile Cloud Computing Application Models". IEEE Communications Surveys Tutorials. 16 (1): 393–413.

[2] Abolfazli, Saeid; Sanaei, Zohreh; Ahmed, Ejaz; Gani, Abdullah; Buyya, Rajkumar (1 July 2013). "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges". IEEE Communications Surveys & Tutorials. 99 (pp): 1–32.

[3] Fangming Liu, Peng Shu, Hai Jin, Linjie Ding, Jie Yu, Di Niu, Bo Li, "Gearing Resource-Poor Mobile Devices with Powerful Clouds: Architecture, Challenges and Applications", IEEE Wireless Communications Magazine, Special Issue on Mobile Cloud Computing, vol. 20, no. 3, pp.14-22, June, 2013.

[4] Abolfazli, Saeid; Sanaei, Zohreh; Gani, Abdullah; Xia, Feng; Yang, Laurence T. (1 September 2013). "Rich Mobile Applications: Genesis, taxonomy, and open issues". Journal of Network and Computer Applications. 40: 345–362.

[5] Khan, A. u R.; Othman, M.; Xia, F.; Khan, A. N. (2015-05-01). "Context-Aware Mobile Cloud Computing and Its Challenges". IEEE Cloud Computing. 2 (3): 42–49. doi:10.1109/MCC.2015.62. ISSN 2325-6095.

[6] Dinh, Hoang T. "A survey of mobile cloud computing: architecture, applications, and approaches". Wireless Communications and Mobile Computing. 13: 1587–1611.