A THEORETICAL MODEL TO PROVIDE SECURITY FOR REMOTE LOCATION AWARE CLOUD DATA CENTRE

Mr. Rakesh Nag Dasari[1*], Dr. G. Rama Mohan Babu[2]

1*. Research Scholar, Department of Computer Science & Engineering,

University College of Engineering,Acharya Nagarjuna University, India.

2. Professor, Department of IT, RVR & JC College of Engineering, India.

Abstract

The growth in the adaptation of the cloud services for various purposes as education, research, social networking, medical research and financial managements is extending the use of cloud based services and client applications to access those services. The client applications can be deployed in various types of devices and this encourages the business scalability for the industry. Hence, the service providers enforces to the policy of allowing access from various devices and locations. These locations or devices are sometimes trusted and most of the situations are untrusted. The cloud based data centres face a major challenge in granting the access for these requests from the client applications. In order to satisfy the business demands, the cloud based data centre providers are forced to allow all access from those applications. Thus, making the data centre virtual infrastructure vulnerable for attacks. The data centres configure various firewall rules to prevent this condition. Nevertheless, these firewalls are static and cannot replace the need for dynamically changing business, application and customer policies with the variable location based access. Hence, the demands from the current researches are to build a dynamic firewall framework to satisfy these needs. This work demonstrates a novel theoretical framework for remote mobile clouds. Another major outcome of this work is to analyse and justify the research requirements for mobile clouds.

Keywords: Mobile Cloud, IoT – Internet of Things, Security measures, firewall

Introduction

The protection issue becomes more complex when we consider attacks from mobile sources. Unlike threats from stationary attackers, mobile attackers disappear from the attack location and resurface elsewhere.A mobile unit frequently changes location, which can introduce inconsistency at a policy level. For example, a mobile user might be subject to a different set of constraints in Hyderabad City than in Delhi, which will affect the data access pattern. Firewall altering schemes must handle such policy changes, due to mobility and other necessary revisions in the policy in real time to eliminate false denial [1].

Mobile clouds support personal and terminal mobility. A mobile unit can mount attacks from any location at any time. Attack packets pass through several gateways before reaching the cloud. Each gateway has its own dynamic firewall, and the cloud is protected by its own firewall [2]. Whenever the policy change is incorporated on any of the firewalls, the change is propagated to all other firewalls for updating.

Nevertheless, the firewalls are configured with a set of rules and none of the packets can be allowed, unless any specific rule allows the packet. The rule configuration for any firewall can lead to few issues, which cannot be ignored in case of a mobile application accessing the data centre, based services [3]:

1. Rules are written at the lower protocol level, a misconfiguration can make the whole intranet unreachable.
2. Rule base might have many redundant rules.
3. Semantics depend not only on the rules, but also on the order in which they're listed, an undesirable feature.

Hence, a dynamic rule based framework to deal with these situations. The rest of the paper is furnished such as in the section – II the cloud mobility and its constraints are been discussed. The next section, Section – III elaborates the outcomes from the parallel researches and focuses on firewall rule development schemes. The Section – IV defines the unsafe location identifications as part of the framework. The further section as Section – V, Section – VI and Section – VII discusses the design of proposed algorithm, model of the proposed framework and conclusion obtained from this work respectively for the establishment of this theoretical framework.

Cloud Mobility

The Mobile Cloud Computing project looks at architectures and protocols of next generation infrastructures that exploit the synergy between Mobile devices, Internet of Things or IoT devices, and Cloud Computing [4]. It develops answers to how to enable new classes of CPU-intensive, and data-intensive, applications for mobile devices and how to process large number of real-time concurrent interactive data streams emerging from the IoT environment [5]. Research areas of interest include formal methods, Operating Systems, Virtualization, and IP-based and Information Centric Networking protocol stacks for resource-constrained environments. Undergoing efforts are summarized below [6].

A. Design robustness using formal language

This effort develops a formal specification using the π-calculus to define a virtual device representation. It also describes a way to compose multiple virtual devices representing physical devices available on the network to build a composite virtual device. During this process we address the offloading of applications running on virtual devices to local clouds (Cloulets) [7]. The proposed 3-tiered (Mobile device, Cloudlet, and Public Cloud) architecture develops a framework to integrate them and case studies to show the structural congruence between a locally executed application and an offloaded version of the same application.

B. Continuous Monitoring

This effort builds on the previous architecture to add continuous performance monitoring from the device perspective [8] [9]. The focus is on collecting data that will supply additional information to improve the performance this dynamic, distributed and real-time nature of the architecture.

C. Protocol for the Interoperability

The application offloading concern is a complex problem, which contains communication, application isolation, and persistence layers. We focus on the first layer – Mobile Offloading Communication Protocol (MOCP). This is a communication protocol between the cloudlet, which plays the server role, and the mobile application manager, which plays the client role. The manager pilots the whole life cycle of the mobile application on the mobile device [10] [11]. An Application Program Interface (API) is built on top of Representational State Transfer (REST) that enables the automatic generation of MOCP's skeletons for servers and mobile devices in multiple programming languages such as Java, C++ and JavaScript.

Thus, understanding the benefits and limitations of the mobile cloud, in the next section this work elaborates the parallel research outcomes on firewall rules.

Review of the Parallel Research Outcomes

The recent research advancements focus on effective firewall designs, as the incoming data packets need to be explicitly accepted by the rule sets. The incoming data packets need to satisfy any specific rule to be accepted in the network.

A model firewall rule is elaborated here [Table – 1].

Rule	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

Table I: Firewall Rule as Result Of Recent Research

The recent research also demonstrates the packet filtration process [Table – 2].

Rule	Dir.	Source Add.	Dest. Add.	Prot.	Source Port	Dest. Port	ACK set	Action
A	In	External	Internal	TCP	> 1023	25	Any	Permit
B	Out	Internal	External	TCP	25	> 1023	Yes	Permit
C	Out	Internal	External	TCP	> 1023	25	Any	Permit
D	In	External	Internal	TCP	25	> 1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

TABLE II: Packet Filter as result of Recent Research

Hence, it is natural to understand that the firewall rules are static in nature and cannot accommodate the dynamic nature of the mobile cloud network.

Thus, this work demonstrates the dynamic firewall policy for client and server side to accommodate the ever-changing cloud mobility security

Proposed Algorithm

In this section of the work, the proposed algorithm is elaborated and compared with the existing methods.

Firstly, the elaboration on the proposed algorithm is carried out [Table – 3]:

```
For all locations
        Select any three landmarks
        For each landmark
                Calculate the delay
                Estimate the distance
                Calculate the region under the landmark
        End For
        Calculate the lowest delay from the data centre from three landmarks
        Make the lowest delay point as primary node
        Calculate the triangular region using three Landmarks
        Calculate the lowest zone among three channels

        If the result is satisfactory
                Then stop
        Else
                Repeat the process
End For
```

TABLE III: Proposed Algorithm for Location Aware Dynamic Rule

Henceforth for the sake of comparison [11] [12], the existing algorithm is furnished here [Table – 4].

```
For all locations
If firewall rule accepts the packet
Take designated action
Else
Reject the packet
End For
```

TABLE IV: EXISTING ALGORITHM - STATIC C FIREWALL RULE SET

Further, the proposed and existing algorithms are analysed visually [Figure – 1] and [Figure – 2].

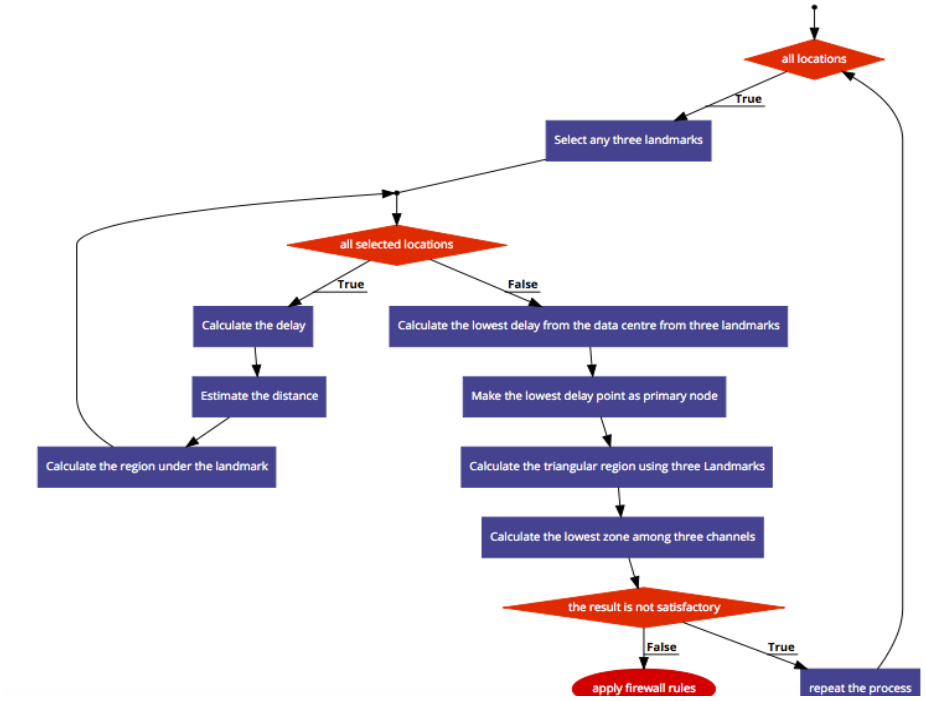

Fig. 1 Process Flow of the Proposed Algorithm

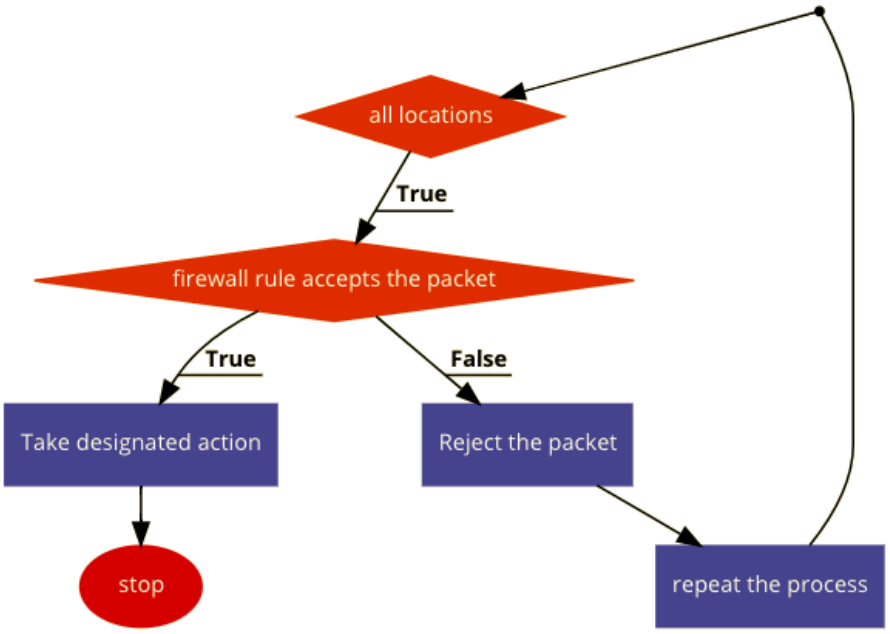

Fig. 2 Process Flow of the Existing Algorithm

Thus in the light of comparative analysis, further this work elaborates the proposed unsafe location awareness component in the next section.

Unsafe Location Identification

The proposed unsafe location identification process is elaborated in this section. When an attacker moves around in a location while attacking the cloud, it will have the same IP address at different points inside the location. To hide their identity and avoid being caught in such movement, attackers generally use a proxy. The tracert (trace route) command, which shows the path an IP packet travelled to reach a destination, isn't helpful because it can't go beyond the proxy. In a mobile network, IP address allocation is dynamic, so it's easy for an attacker to spoof an IP address and mount an attack through a proxy.

As a security measure, the system maintains location area codes of unsafe locations and discards incoming packets from these unsafe locations without even analysing them. To determine if a location is safe or unsafe, the system records the number of attacks from each known location. If the number of attacks from a particular location reaches a threshold, it marks the location as unsafe. It's an ongoing process of marking unsafe locations based on the number of attacks originating from a specific location. It is proposed to maintain and update a database of unsafe locations continuously.

With the proposed algorithm and the unsafe location identification process, now it is the demand of the practice to propose a framework to implement the novel method. Hence, in the next section, this work elaborates the framework.

Proposed Framework

The proposed framework is to adapt to the dynamic process policy management framework to capture the safe, unsafe and partially safe or partially unsafe locations. The framework is furnished here [Figure – 3].

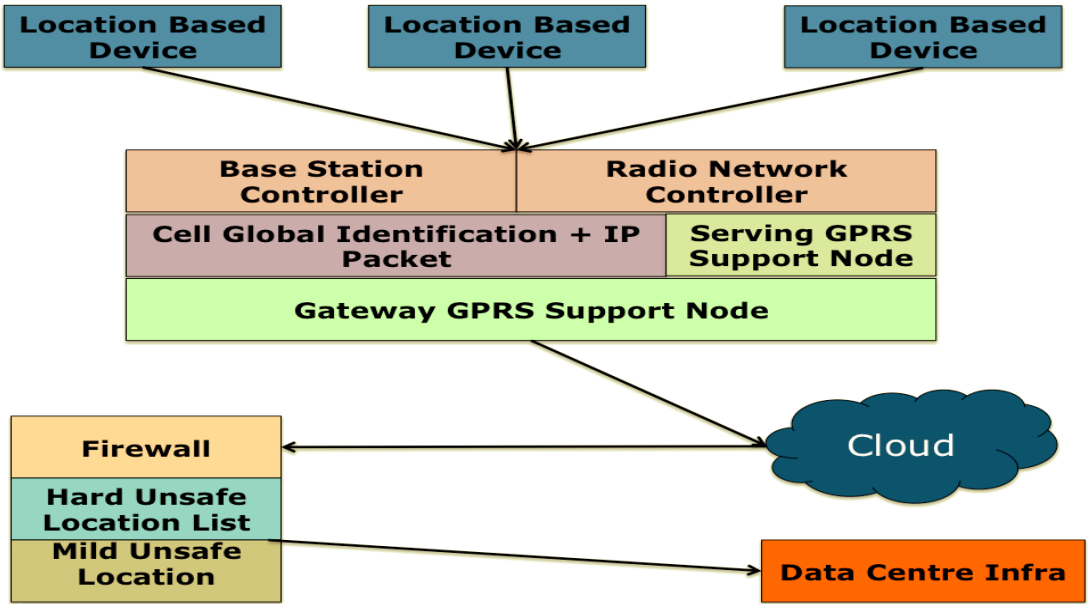

Fig. 3 Proposed Framework

Because this proposed approach could identify the location of the attackers, it compromises the attacker's privacy. Although this is not an issue in the case of an attacker, this scheme should be able to protect the privacy of a typical user if that user's actions look like an attack.

Thus this work proposes the conclusions in the next section with the complete knowledge of existing algorithm, proposed algorithm and proposed framework.

Conclusion

The proposed framework and the deployed proposed algorithm defines new dimensions in the space of cloud security for mobile cloud service environments. This work demonstrates a novel approach to determine safe and unsafe locations based on the amount of attacks generated from those locations. The proposed solution can make the data centre providers free from access request analysing aspects, the service providers liberated from non-access issues by their clients and clients from the trusted factor issues, making the mobile cloud computing enrich in terms of better service enhancements.

References

[1] S. Jajodia et al., "Flexible Support for Multiple Access Control Policies," ACM Trans. Database Systems (TODS), vol. 26, no. 2, 2001, pp. 214–260.

[2] I. Cervesato et al., "Relating Strands and Multiset Rewriting for Security Protocol Analysis," Proc. 13th Computer Security Foundations Workshop (PCSFW 00), 2000, pp. 35–51. F.J.

[3] Fabrega, J.C. Herzog, and J. Guttman, "Strand Spaces: Why Is a Security Protocol Correct?" Proc. IEEE Symp. Security and Privacy, 1998, pp. 160–171.

[4] J. Loeckx and K. Sieber, The Foundations of Program Veri cation, John Wiley & Sons, 1987.

[5] V. Kumar, Mobile Database Systems, John Wiley & Sons, 2006.

[6] H. Seki, "Unfold/Fold Transformation of Stratified Programs," Theoretical Computer Science, vol. 86, no. 1, 1991, pp. 107–139.

[7] Cisco ISO Lock and Key Security, white paper, Cisco Systems, 1996.

[8] Y. Bartal et al., "Firmato: A Novel Firewall Management Toolkit," Proc. IEEE Symp. Security and Privacy, 1999, pp. 17–31.

[9] A. Mayer, A. Wool, and E. Ziskind, "Fang: A Firewall Analysis Engine," Proc. IEEE Symp. Security and Privacy, 2000, pp. 177–187.

[10] S. Ioannidis et al., "Implementing a Distributed Firewall," Proc. ACM Conf. Computer and Comm. Security, 2000, pp. 190–199.

[11] E. Goren and O. Duskin, "Mobile Firewall," internal report, Check Point Software Technologies, Hebrew Univ.

M. Gondree and Z.N.J. Peterson. "Geolocation of Data in the Cloud," Proc. 3rd ACM Conf. Data and Application Security and Privacy, 2013.