International Journal of Computer and Communication Technology

Volume 7 | Issue 4 Article 14

October 2016

IMPROVED SECURITY SYSTEM IN MOBILE CLOUD ACCESS THROUGH FUZZY INTRUSION DETECTION TECHNIQUE

S. GOWRI
Department of Computer Science & Engineering , Angel College of Engineering and Technology, Tirupur-India, gowri1666@gmail.com

A.NAVEEN KUMAR
Department of Computer Science & Engineering , Angel College of Engineering and Technology, Tirupur-India., gpatangel@gmail.com

A.NAVEEN KUMAR
Department of Computer Science & Engineering , Angel College of Engineering and Technology, Tirupur-India., anaveenkumar@gmail.com

M. SASITHARAGAI
Department of Computer Science & Engineering , Angel College of Engineering and Technology, Tirupur-India., sasitharagai@gmail.com

IMPROVED SECURITY SYSTEM IN MOBILE CLOUD ACCESS THROUGH FUZZY INTRUSION DETECTION TECHNIQUE

S. GOWRI[1], T.GNANAPRAKASAM[2], A.NAVEEN KUMAR[3] & M.SASITHARAGAI[4]

[1,2,3&4]Department of Computer Science & Engineering , Angel College of Engineering and Technology, Tirupur-India.
Email:gowri1666@gmail.com,gpatangel@gmail.com,anaveenkumar@gmail.com,sasitharagai@gmail.com

Abstract - Mobile phones are playing a vital role in every one's life. The computing strategy of mobile internet usage is lower than the mobile usage, this may due to the security threat. In general mobility and cloud computing initializing the global marketing, sales and development activities using mobile platforms to market and sell products and services. Mobile/Cloud computing is about improving internal efficiencies and productivity and improving your sales and marketing channels and reach. So we need to provide the security for the efficient mobile cloud access. In this proposal, a fuzzy based intrusion detection technique. This enhances the vulnerable security system for the mobile cloud users.

Keywords: *Mobile Cloud, Fuzzy, Vulnerable, Mobile platforms*

I.INTRODUCTION

Computing resources are owned and managed by a cloud service provider (CSP). Using virtualization techniques, these virtualized resources, such as hardware, platforms, or services, are dynamically allocated to scale on demand according to customers' needs. If a CSP fails to offer the demand, the CSP may outsource to other CSPs[2]. It's easy to see that cloud computing is simply the next immense step in the evolution of the internet. We, as consumers of information services, have moved from mainframe to desktops to mobile devices such as tablets, smart phones. An emerging computer paradigm where Content and services reside in massively scalable Content centers in the cloud and can be accessed from any connected devices over the internet. The concept of Mobile Cloud Computing (MCC) be going to make the advantages of Cloud Computing available for mobile users but will provide additional functionality to the cloud as well.

1).General Model of Cloud Computing

a. Software as service

Customer rents computing resources instead of buying and installing them in their own data center[3].

Advantages: Rapid start-up, maintenance and upgrades performed by the vendor, scalable.

Risks: Minimal customization, data integration, security and privacy, no control over upgrades, exit strategy, Proliferation.

Examples: Salesforce.com, Google Apps.

•Amazon's Elastic Compute Cloud (Amazon EC2)

b.Platform as a Service

Solution stack - An integrated set of software that provides everything a developer needs to build an application for both software development and runtime.

Advantages: Focus on high value rather than infrastructure, economies of scale, Provides Scalable go-to-market capability.

Risks: Exit strategy, pricing model, upgrade issues.

Examples: force.com, Microsoft Azure, web and e-mail Hosting, Google App Engine, AppJet, Etelos, Qrimp, and Force.com

c.Infrastructure as a Service

Business applications that are hosted by the provider and delivered as a service.

Advantages: Scalable, rapid start-up, peak leveling.

Risks: Pricing model, potential lock-in, security and privacy, proliferation

Examples: Amazon EC2, Rack space, Sales force .com

2).Comparison of Grid Computing and Cloud Computing

Both are scalable & shareable the Resources and usability of the resource is high. Grid is used for batch-style job execution, such as a scientific calculation, whereas the cloud serves long-lasting services and X as a service (XaaS).Loose coupled cloud infrastructure empowers developers to unfold their creativity.

3).Comparison of cluster computing, Grid Computing and Cloud Computing in security

Cluster	Grid	Cloud
Traditional login/password-based.	Public/private key pair based authentication and mapping	Each service provided with a virtual machine.
Medium level of privacy	a user to an account. Limited	High security/privacy

depends on User privileges.	support for privacy.	is guaranteed. Support for setting per-file access control list (ACL).

Table1: Cluster Vs Grid Vs Cloud

4).Intrusion Detection System

An intrusion detection system monitors network traffic and/or monitors host audit logs in order to determine whether any violations of an organization's security policy have taken place. IDS can detect intrusions that have circumvented or passed through a firewall or that are occurring within the local area network behind the firewall. A networked system's security policy should require that designated system and network administrators and response team members are trained in the use of intrusion response tools and environments. Also, the policy should require that the inventory of all applications software[4], operating systems, supporting tools, and hardware be kept up to date, and quick access to backups in an emergency is required, even if they are stored at a remote site. This may include defining procedures that give specific managers the responsibility to authorize such access.

Intrusion detection (ID) processes must be planned and implemented to help organizations detect and respond to incidents before they occur. It's important to respond to incidents in an efficient and effective manner. For example, the information system security officer (ISSO) must determine how the organizations going to monitor the intrusion detection system[5], who will monitor it, how alerts will be processed, and how the incident is remediated and with what level of response.

The most common approaches to ID are statistical anomaly detection (also known as behavior-based) and pattern-matching (also known as knowledge-based or signature-based) detection.

II. SIGNIFICANT AREAS FOR CLOUD COMPUTING

1. cloud Security Challenges

Areas for security concerns in cloud computing are[2,3]

a. Securing data at rest.

Cryptographic encryption is certainly the best practice in worldwide, it's the law for securing data at rest at the cloud provider. Auspiciously, hard drive manufacturers are now shipping self encrypting drives that implement the TCG's(Trusted Storage standards). Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Software encryption can also be used, but it is slower and less secure since the encryption key can be copied off the machine without detection.

b Securing data in transit.

Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit. Well-established protocols such as SSL/TLS should be used here. The tricky part is strong authentication, as described next.

c Access Control and Authentication.

User authentication is often the primary basis for access control, keeping the bad users out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The TPM[6] can easily provide stronger authentication than username and passwords. TCG's IF-MAP standard allows for real-time communication between the cloud provider and the customer about authorized users and other security issues. When a user is fired or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within seconds. If the fired user is logged into the cloud, they can be immediately disconnected. Trusted Computing enables authentication of client PCs and other devices, which also is critical to ensuring security in cloud computing.

d.Separation between customers.

One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs)[4,5] and a hypervisor to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation. In addition, the TPM can provide hardware-based verification of hypervisor and VM integrity. The TNC architecture and standards can provide strong network separation and security.

e. Cloud legal and regulatory issues.

To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy[7]. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, Trusted Storage and TPM access techniques can play a key role in limiting access to data.

f. Incident response.
As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response or at least automated notification is the best solution. TCG's IF-MAP (Metadata Access Protocol) specification enables the integration of different security systems and provides real-time notification of incidents and of user misbehavior.

III.RELATED WORK

A. Trusted data sharing over untrusted cloud storage providers

Fig 1 specifies the specific security requirements for securing data storage in the cloud can be summarized as follows:

1. Data stored on the cloud should be kept private and the cloud storage provider should not be able to compromise the data Confidentiality by any means.
2. The data owner has full control over authorization of data sharing. With authorization given by the owner, the designated user can then access the data kept on the cloud. Nevertheless, the process should not give the cloud provider any right to access the data.

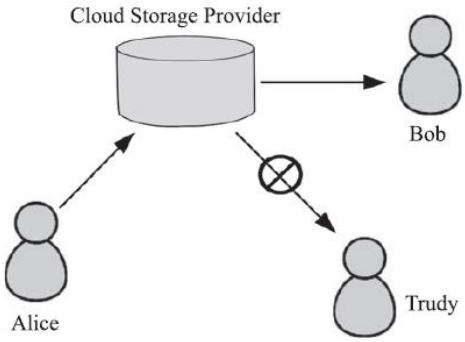

Fig1: Secure sharing on cloud [4].

There are still some grey areas that need to be addressed, such as security and privacy of user's data stored on cloud server(s), security threats caused by multiple virtual machines, and intrusion detection. As MCC is based on cloud computing so all the security issues are inherited in MCC with extra limitation of resource constraint mobile devices. Due to resources limitation, the security algorithms proposed for cloud computing environment cannot be directly run on mobile device[8]. There is a need of lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices.

B. A Security Framework for Efficient and Secure Data Storage Services in MCC

Zhou et al. [5] proposed a privacy preserving framework called Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) for lightweight mobile devices. The proposed scheme offloads the processing and storage intensive encryption and decryption operations on cloud without revealing any information about data contents and security key

Fig 2 represents the Data Owner (DO) can be a mobile device or a sensor that may request to store and retrieve data from cloud. To increase the processing capability of DO, major portion of encryption and decryption operations are outsourced on cloud. Encryption Service Provider (ESP) encrypts the file for DO without having knowledge about the security keys.

Decryption Service Provider (DSP)[8] decrypts the file for DO without getting any information about data contents. The encrypted data is stored on storage service provider. Authors assume that Trusted Authority (TA) is responsible to generate and distribute keys among DOs.

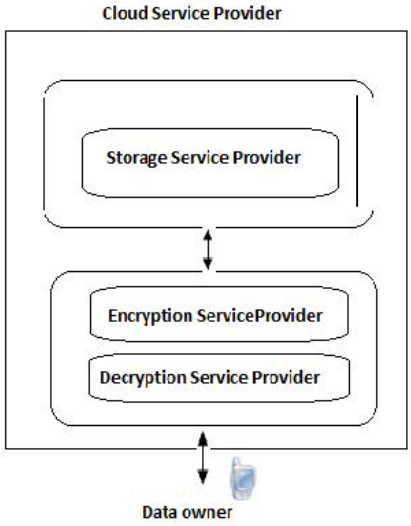

Fig 2: Traditional Cryptography

For example, Soghoian [7] believes that the likely reason Google took several years to offer HTTPS (Hypertext Transfer Protocol Secure), an industry standard encryption protocol, by default is the issue of cost because encryption takes processing power and memory. Plainly download all the encrypted data, decrypt and search on local computers is not practical.

IV. FURTHER WORK

The advantages of cloud computing can become disadvantages. Although the cloud providers can afford and might implement better security mechanism into their systems than the common end-users, like hiring security experts and installing anti-

virus software, the facts of remote access, virtualization, platform sharing, border crossing, lack of data control, and massive use of third party services and infrastructures all make security and privacy a major worry.

Fig 3 represents, a Rule-based intrusion detection system, an attack can either be detected if a rule is found in the rule base or goes undetected if not found. The attacks that are found by the RIDS are blocked here.

Fuzzy Intrusion Detection System is used in order to make accurate predictions from the results of Rule-based IDS. In a Rule-based intrusion detection system, an attack can either be detected if a rule is found in the rule base or goes undetected if not found. The output of the RIDS goes to the Fuzzy component of FASIDS[9] for further analysis (Susan M. Bridges 2002) (Ambareen Siraj et al 2001) using fuzzy Cognitive Mapping(FCM).

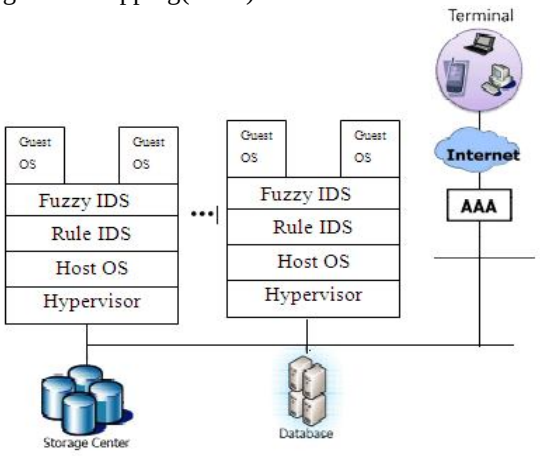

Fig 3: Security through using FIDS

A. Algorithm for Fuzzy Intrusion Detection System

Step 1 : Let x= number of login failures and t= time interval

Step 2 : x=normalization of (x)=(x-*min*)/(*max*-*min*)

where,

min is the minimum value for the attribute that x belongs to *max* is the maximum value for the attribute that x belongs to Step 3 : The output of the fuzzification is given to FCM which has the Fuzzy rules in the form: IF condition THEN consequent Suspicious event Where, Condition is a complex fuzzy expression i.e., that uses fuzzy Consequent is an atomic Expression

V.CONCLUSION

In this rule based semantic intrusion detection system Misuse detection uses rule based IDS that follow a signature-match approach which is time consuming. Proposed has an efficient memory usage since the amount of memory needed for working of the IDS depends on the rule table size. The complexity ratio of the memory usage and data consumption is very lower in this proposed technique. In further, we will enhance this in the all the kinds of cloud based applications in the mobile environment.

REFERENCES

[1] www.trustedcomputinggroup.org/

[2] Ambareen Siraj, Susan M. Bridges and Rayford B. Vaughn (2001), 'Fuzzy Cognitive Maps For Decision Support In An Intelligent Intrusion Detection System', In the proceedings of 20th International Conference of North American fuzzy information (NAFIPS), vol. 4,pp.2165-2170.

[3] R. Buyya, R. Ranjan, Federated Resource Management in Grid and Cloud Computing Systems, Future Generation Computer Systems, 26 (8) (2006) 1189-1191

[4] Rong Chunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer Networks (IWSCN 2011); 2011.

[5] Z. Zhou, D. Huang, Efficient and Secure Data Storage Operations for Mobile Cloud Computing, IACR Cryptology ePrint Archive: 185 (2011).

[6] H. Canepa, D. Lee, A Virtual Cloud Computing Provider for Mobile Devices, in: Proc. 1st ACM Workshop on Mobile Cloud Computing & Services Social Networks and Beyond (MCS '10), San Francisco, USA, June 2010.

[7] Soghoian, C. Caught in the cloud: privacy, encryption, and government back doors in the Web 2.0 Era, J on Telecomm & High Tech L 2009, 8: 359 – 424.

[8] Z. Zhou, D. Huang, Efficient and Secure Data Storage Operations for Mobile Cloud Computing, IACR Cryptology ePrint Archive: 185 (2011).

[9] Distributed Intrusion Detection in Clouds Using Mobile Agents, 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences

VII. AUTHORS BIOGRAPHY

Ms. S.Gowri received B.E degree in Computer Science and Engineering from Anna University, Coimbatore and pursuing her M.E degree in Computer Science and Engineering from Anna University, Chennai. She has published 4 papers in National conferences. She has attended various Seminars, Workshops to enhance her knowledge. She is a life time member of IAENG.

Mr. T. GnanaPrakasam received M.E degree in Computer Science & Engineering from Anna University, Coimbatore. Now pursuing his Ph. D in Open Source Mobile Cloud Computing from Anna University, Chennai. He is the Open Source Club in charge of Angel College of Engineering and Technology; he attended more than 15 national and international level workshops. Also he has organized two national level conferences.

Mr. A.Naveen kumar received B.E degree in Computer Science and Engineering from Anna University, Coimbatore and pursuing his M.E degree in Computer Science and Engineering from Anna

University, Chennai. He has published 4 papers in National conferences. He has attended various Seminars, Workshops to enhance her knowledge.

Ms. M.Sasitharagai received B.E degree in Computer Science and Engineering from Anna University, - Coimbatore and pursuing her M.E degree in Computer Science and Engineering from Anna University, Chennai. She has published 3 papers in National conferences and 1 paper in International conference. She has attended various Seminars, Workshops to enhance her knowledge. She is a life time member of IAENG.