ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Study of Mobile Cloud Computing Security against Cyber Attacks

Miss. Ankita S. Koleshwar
Research Scholar
Amravati, India
ankita.koleshwar12@gmail.com

Mrs. S. S. Sherekar
Dept. of Computer Science and Engg, SGB Amravati
University, SGB Amravati University, Amravati, India
ss_sherekar@rediffmail.com

V.M. Thakare
Dept. of Computer Science and Engg,
SGB Amravati University, Amravati, India
vilthakare@yahoo.co.in

Abstract : Network security involves all the performance that organizations, institutions agree to protect the value and ongoing usability of resources and the reliability and continuity of operations. The attacks like Sybil, Vampire, Phishing and lot more are affecting the performance of the systems. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to fight them. There are three ways to deal with attacks in network that are Detection, Prevention and Counter Measures which are studied in this paper which ultimately support to improve the security.

Keywords: Sybil Attack, Phishing Attack, Vampire Attack.

I. INTRODUCTION

In the security world, there is one structure of Confidentiality, Integrity and Availability it is recognized as CIA Triad, these three ethics are pertinent diagonally the whole area under discussion of Security Analysis, [1] from access to a user's internet history to security of encrypted data across the internet. If any one of the three can be breached it can have serious consequences for the parties concerned. This structure is for ensuring that each organization must be secured enough to run their operations.

[2]They become the building blocks that must be used in designing a secure system which applies to three categories of assets that are data, software and hardware resources. Some types of security attacks attempt to disagree with accessing the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. Security indicates the need for protecting information from unauthorized access, use, exposure, interruption and variation [3].

Likewise, there are various attacks which are very dangerous for the users who are on cloud. For the security point of view, attack prevention is very necessary. The attacks like Sybil, Vampire, Phishing and lot more are affecting the performance of the systems. And now the security approach should be effective
against new kind of attacks.

II. ATTACKS A. SYBIL ATTACK

Sybil attack is a type of attack in which an attacker manages to create and control more than one identity on a single physical device and it is a particularly harmful attack in sensor networks. To put off this attack, Sohail Abbas et. al [4] present a scheme which helps in detection of Sybil identities. This scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities.

There are two ways to validate an identity in Sybil [5]. The first type is Direct validation, in which a node directly tests whether another node identity is valid. And the second type is Indirect validation, in which nodes that have already been verified are allowed to assure for other nodes.

There are several novel methods by which a node can verify whether other identities are Sybil identities, including radio resource testing, key validation for rando key predistribution, position verification and registration.

The random key distribution will be used in many scenarios for secure communication.

A. *Vampire Attack:*

“Vampire” attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. In Eugene Y. Vasserman et. al [6] explores in the research that is resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power. Vampire attack is the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers.

The strength of the attack is measured by the ratio of network energy used in the begin case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant.

B. *Phishing Attack:*

Phishing is a social engineering attack that aims at exploiting the weakness found in system processes as caused by system users. According to PhishTank “Phishing is a fraudulent attempt, usually made through email, to steal your personal information [7].

There are two types of detection approaches in mitigation of phishing attacks and that are, first is user training approach and second is software classification approach. These both detection techniques not only help in directly protecting end-users from falling victims to phishing campaigns, but can also help in enhancing phishing honeypots to isolate phishing spam from non-phishing spam.

C. Epidemic Attack:

Epidemic Attack is a severe security problem in network-coding-enabled wireless mesh networks (WMNs). Yongkun Li et. al [8] provide a ceremonial analysis to quantify the performance of the algorithms and present a set of fully distributed defense and detection algorithms to address the pollution attack problem in wireless mesh networks that are configured with network coding enabled opportunistic routing protocol with proposing a general detection algorithm that can not only detect attackers even if cooperative pollution attack is launched, but also speed up the detection.

D. Snoop-Forge-Replay Attack:

The Snoop-Forge-Replay is a sample-level forgery attack and is not specific to any particular keystroke-based continues verification method or system. In Khandaker A. Rahman et. al [9] present a result from 2640 experiments which shows that the snoop-forge- replay attacks achieve alarmingly high error rates compared to zero-effort fraud attacks, which have been the *de facto* standard or evaluating keystroke-based continues verification systems.

E. Cyber Attack:

In [10] introduces new analytical techniques for performing vulnerability analysis of state estimation when it is subject to a hidden false data injection cyber-attack on a power grid's SCADA system. In this research, an algorithm based on graph theory which allows determining how many and which measurement signals an attacker will attack in order to minimize his efforts in keeping the attack hidden from bad data detection.

F. Timing Attack:

Sometimes, even though software is functionally secure, information can be deduced about secret data from the timing- behavior of a system [11]. For example, a password-checking function written in a particular way might take a time corresponding to how close the guess was to the actual password, and in this way there is a security leak which may eventually be exploited. The Timing attack can often reduce the number of authentication requests required for a successful guess by an order of enormity.

G. DDoS Attack:

Virtual Machines are use to provide computational infrastructure and services to organizations is increasingly widespread in the modern IT industry. Today, virtualization technologies can be found in almost every data center. However, it remains unknown whether the VMs are more vulnerable on external malicious attacks. In Ryan Shea et. al [12] present a study on the performance of modern virtualization solutions under networked denial of service (DoS) attacks.

In Jerome Francois et. al [13] focuses on the problem of DDoS attacks and present the theoretical foundation, architectureand algorithms of *FireCol*. Specially they focuses on exclusively on flooding DDoS attacks. *FireCol* is a new collaborative system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source(s) at the Internet service provider (ISP) level.

III. METHODOLOGIES

The following section discusses the structure of various attacks and its working implementation with testing the attack to fight against the problem.

A. Sybil Attack :

The RSS-based detection mechanism is used to protect the network against Sybil attacks. This design worked on the MAC layer using the 802.11 protocol without the need for any extra hardware.

In Sohail Abbas et. al [4] proposed scheme, the "Sun Spot Testbed" is conducted. The aim of using this testbed is to check the entrance and exit behavior of a node from RSS values. The Simulator used in [4] is Network Simulator NS-2.30 and it focused on some attributes of the network that are mainly responsible for affecting the accuracy of Sybil attack detection scheme.

These attributes are number of network connections, node density and transmission rate. Simulation Parameters used are like Area, Speed, Pause time, Number of nodes, MAC 802.11, Packet size, Simulation time, Malicious population, Sybil Ids per malicious node etc.

The two metrics are determined while detecting the accuracy of the scheme in different environments. The first is True Positive Rate (TPR) and second is False Positive Rate(FPR). They are formulated as follows –

True Positive Rate = <u>Correctlydetectedwhitewashids</u>
Total whitewash ids

False Positive Rate = <u>Incorrectlydetectedgoodids</u>
Total good ids

The simulation result showed that the scheme works better even in mobile environments and can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy.

B. Vampire Attack :

In Eugene Y. Vasserman et. al [6] introduces the no-backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space and wishing for defenses against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets and presenting a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience with introducing two different attacks.

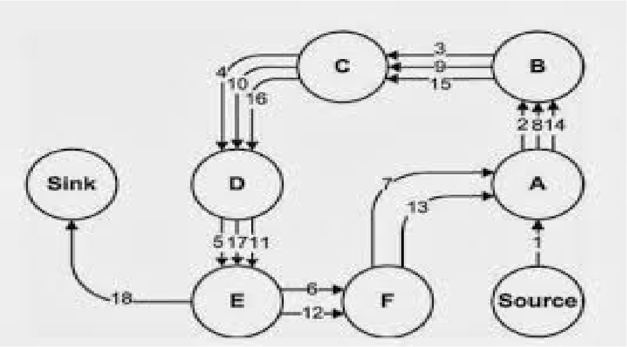

Figure. (a) Carousel attack

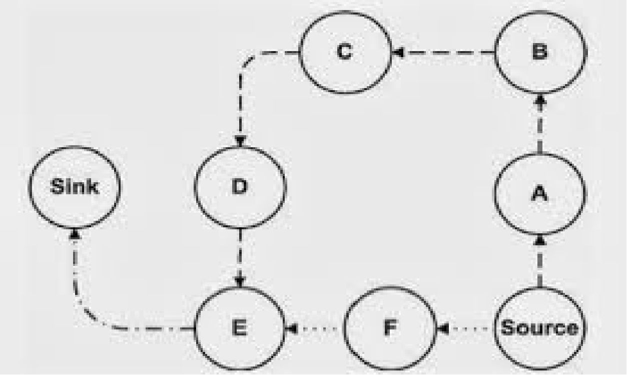

Figure. (b) Stretch attack

In the first attack, an adversary composes packets with purposely introduced routing loops and named as the carousel attack, since it sends packets in circles as shown in above fig. (a). And in second attack, according to fig. (b), also targeting the source routing, an adversary constructs artificially long routes, potentially traversing every node in the network and named as stretch attack.

This research presents the Attacks on Stateless Protocols and Stateful Protocols and proposed defenses against some of the forwarding-phase attacks.

C. *Phishing Attack:*

In Mahmoud Khonji et. al [7] focused on the Human factor, which will present some of the work contributed in the field of user training in relation to phishing attacks with presenting some Phishing detection techniques named as follows.

a. ***Phishing Detection by Blacklists*:** Blacklists are frequently updated lists of previously detected phishing URLs, IP address or keywords. Blacklists do not provide protection against zero-hour phishing attacks as a site needs to be previously detected first in order to be blacklisted. The applications which are enclosed in Phishing detection by Blacklists are as follows –

a) *Google Safe Browsing API*
b) *DNS-Based Blacklist*
c) *PhishNet: Predictive Blacklisting*
d) *Automated Individual White- List*

b. ***Phishing Detection by Heuristics*:** Phishing heuristics are characteristics that are found to exist in phishing attacks in reality, however the characteristics are no guaranteed to always exist in such attacks. If a set of general heuristics tests are identified, it can be possible to detect zero-hour phishing attacks, which is an advantage against blacklists. This includes

a) SpoofGuard
b) Collaborative Intrusion Detection
c) PhishGuard : A Browser Plug-in
d) PhishWish : A Stateless PhishingFilter using Minimal Rules
e) CANTINA : A Content- Based Approach
f) A Phishing Sites Blacklist Generator

***c. Phishing Detection by Visual Similarity*:** In detection of Phishing attack by Visual Similarity, a number of proposed solutions that attempt to detect Phishing attacks based on Visual appearance, as opposed to analyzing the underlying source code or network level information.

This includes the following mechanisms –

a) Classification with Discriminative Keypoint Features
b) Visual Similarity-based Detection without Victim Site Information

d. Phishing Detection by Data Mining **:** The Phishing detection in Data mining is considered as a document classification or clustering problem, where models are constructed by using Machine Learning and Clustering algorithms etc.

The wrapping up of phishing attack detection in this research as listed above reviewed a number of anti-phishing software techniques.

D. *Epidemic Attack:*

In Yongkun Li et. al [8] proposed a randomized and fully distributed detection mechanism, present a general analytical framework to quantify the performance of detection algorithms that shows the effectiveness and efficiency of the algorithms. Validation of this analytical models are given via extensivesimulationsand system prototype. The simulation results shows the accuracy of models and the effectiveness and the efficiency of the algorithms.

In randomized and fully distributed detection mechanism, any legitimate node in a WMN can execute detection algorithms to identify its malicious neighbors and allowing malicious nodes to pretend as legitimate nodes and cooperatively inject polluted packets. The detection methodology is based on batch verification to identify pollution attackers, as well as the analytical methodology to quantify the performance measures of the algorithms. It includes –

a) Core Idea of the Detection Algorithms
b) Attackers with Imitation Probability $\delta = 0$
c) Attackers with Imitation Probability $\delta > 0$
d) Improvement on *Pfn*

This research provides a formal analysis to quantify the performanceof detection algorithms, and extensive simulations are provided to validate the theoretic analysis and shoe the effectiveness and efficiency of the detection algorithms.

E. *Snoop-Forge-Replay:*

In Khandaker A. Rahman et. al [9] presents a new sample-level attack called "Snoop-Forge-Replay" attack that synthesizes keystroke forgeries using timing information stolen from victim users. Snoop-Forge-Replay attack is surprisingly effective when a small amount of Snooped latencies are used to build forgeries. *(Few words become deadly).*

The parameters for Snoop-Forge-Replay Attack are as follows.

a) Length of Snooped Text :
b) Gaussian Perturbation of Snooped Latencies
c) Filtering Outliers
d) Minimum Frequency of Digraphs in the Snooped text

F. *Cyber Attack:*

In Gabriela Hug et. al [10] research, the AC and DC State Estimation is given for mathematical dependencies. In AC State Estimation, nonlinear mathematical dependency formulated as –

$$\mathbf{z = h(x) + e}$$

And in the DC State Estimation, linear relationships between measurements and state variables given as –

$$\mathbf{z = Hx + e}$$

In the research [10], IEEE 57 bus system is used as the test system. It is assumed

that the measurements taken in the system are as follows –

a) Active power flows on all lines at both ends of the line,
b) Reactive power flows on all lines at both ends of the line;
c) Voltage magnitudes at all buses;
d) Voltage angles at all buses etc..

Analysis of the implications of a hidden false data injection attack at the RTU level on ac state estimation have been derived and a method has been presented that determines the number of measurements an attacker needs to modify in order to prevent the detection of those modifications for any given system.

The research present a Smart grid network architecture which is the necessary communication platform for monitoring and controlling the grid operation. Four Smart Grid Cyber Attacks like Device attack, Data attack, Privacy attack and Network availability attack that exist the fundamental security techniques for defending the above mentioned cyber attacks in smart grid communication networks. The techniques are –

a) Access Control
b) Authentication
c) Privacy Preservation
d) Intrusion Detection

The above techniques are used in [10] research to overcome the security problem.

G. *DDoS Attack:*

Jerome Francois et. al [12], [13] present a *FireCol* Architecture, a scalable solution for the early detection of flooding DDoS attacks.

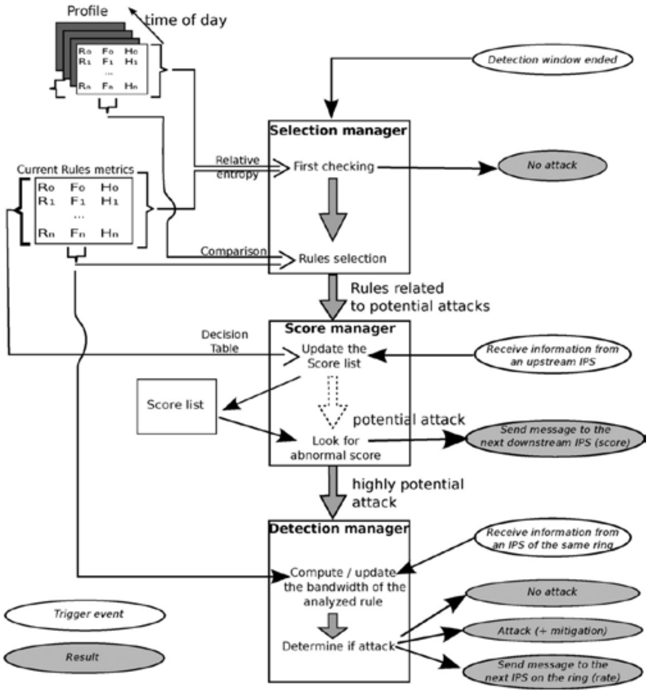

Figure: FireCol System Architecture

a. ***Ring-Based Overlay Protection*:** The *Fire Col* system maintains virtual rings or shields of protection around registered customers.
b. ***Subscription Protocol***: *FireCol* protects subscribers based on defined rules. A *FireCol* rule matches a pattern of IP packets. *FireCol* is an added value service to which customers subscribe using the protocol.
c. ***Multiple Customers*:** Because of inherent complete independence, *FireCol* allows the coexistence of multiple virtual protection rings for multiple customers across the same set of IPSs.

This research presents an *FireCol* Attack Detection Algorithm which is –

Algorithm 1 : checkRule (IPS_id, *i*, rate*i*, cap*i*) For the mitigation shield, the algorithm is used –

Algorithm 2 : mitigate (*ri*, firstRing)

When an attack is detected, *FireCol* rings form protection shields around the victim. In order to block the attack as close as possible to its source(s), the IPS that detect the attack informs its upper-ring IPSs, which in turn apply the vertical communication process and enforce the protection at their ring level.

After the detection and mitigation of an attack against some host *h*, *FireCol* continue the detection process looking for some additional attack sources.

This research mainly used a simulation-based approach for the evaluation of the *FireCol* system.

IV. PERFORMANCE EVALUATION

The RSS based detection mechanism is presented for the Sybil attack problem in the network. RSS-based detection mechanism gives the better result for protecting the network from Sybil attack. The research on Vampire attack presents the Attacks on Stateless Protocols and Stateful Protocols and proposed defenses against some of the forwarding-phase attacks.

The only means of preventing phishing attacks is to alert the dealing that may be spoofed and the person who might become the victim of such an attack. The study of Epidemic attack provides a formal analysis to quantify the performance of the algorithms and show the effectiveness and efficiency of the detection algorithms.

The study of Snoop-Forge-Replay present a result from 2640 experiments which shows that the snoop-forge-replay attacks achieve alarmingly high error rates compared to zero-effort fraud attacks, which have been the *de facto* standard or evaluating keystroke- based continues verification systems. The research of Cyber attack gives the model which incorporates a method for automated attack generation given the network configuration, characteristics describing hacker capabilities, and vulnerabilities of the network. The study of DDoS attacks suggests the network providers can reduce a substantial volume of malicious traffic with targeted deployment of DDoS defences.

The structure and behavioral pattern of each of the attack is different. So we need to study the behavioral pattern to identify the attack and take the measures accordingly.

V. CONCLUSION

Mobile Cloud Computing offers the various services in very sensitive fields such as financial sector, banking, on line payments and all types of on-line transactions, which demands the critical security related vulnerabilities within the mobile cloud computing platform. Nothing on the Internet is completely secured and even the biggest players suffer from serious attacks and security breaches.

The study is necessary on different types of attacks to improve the security on Mobile Cloud Computing. Specifically, how different attacks affect the performance of the network and find out the security measures which have not solved up till now. The technology is constantly changing, and making a challenging task for researchers and hence we need this study to restrict the attacks and to improve the security.

VI. REFERENCES

[1]. Todd Kennedy, Ray Hunt, “A Review of WPAN Security: Attacks and Prevention”, ACM, pp. 10-12, September 2008.

[2]. Jingguo Wang, Nan Xiao, H. Raghav Rao, “Drivers of Information Security Search Behavior: An investigation of Network Attacks and Vulnerability Disclousures”, ACM Transactions on Management, Information Sysytems, Vol. 1, No.1, December 2010.

[3]. Mukesh Singhal, Santosh Chandrasekhar, Tingjian Ge, R. Sandhu R. Krishnan, Gail-Joon Ahn, Bertino E., "Collaboration in multicloud computing environments: Framework and security issues," IEEE Transactions on *Computer* , Vol.46, no.2, pp.76,84, Feb. 2013.

[4]. Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, Kashif Kifayat, “Lightweight Sybil Attack Detection in MANETs”, IEEE Journal on Systems, Vol. 7, No. 2, pp. 236- 248, June 2013.

[5]. Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, Wade Trappe, “Channel-Based Detection of Sybil Attacks in Wireless Networks”, IEEE Transactions On Information Forensics And Security, Vol. 4, No. 3, pp. 492-503, September 2009

[6]. Eugene Y. Vasserman, Nicholas Hopper, “Vampire Attacks: Draining Lifefrom Wireless Ad Hoc Sensor Networks”, IEEE Transactions on Mobile Computing, Vol. 12, No. 2, pp. 318-332, February 2013.

[7]. Mahmoud Khonji, Youssef Iraqi, Andrew Jones, “Phishing Detection: A Literature Survey”, IEEE Communications on Surveys & Tutorials, Vol. 15, No. 4, pp. 2091-2121, Fourth Quarter 2013.

[8]. Yongkun Li, John C. S. Lui, “Epidemic Attacks in Network-Coding-Enabled Wireless Mesh Networks: Detection, Identification, and Evaluation”, IEEE Transactions On Mobile Computing, Vol. 12, No. 11, pp. 2219-2232, November 2013.

[9]. Khandaker A. Rahman, Kiran S. Balagani, Vir V. Phoha, “Snoop-Forge-Replay Attacks on Continuous Verification With Keystrokes”, IEEE Transactions On Information Forensics And Security, Vol. , No. 3, pp. 528-541, March 2013.

[10]. Gabriela Hug, Joseph Andrew Giampapa, “Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks”, IEEE Transactions on Smart Grid, Vol. 3, No. 3. pp. 1362-1370, September 2012.

[11]. Adrian Hayes, “NetworkService Authentication Timing Attacks”, IEEE Crypto Corner on Computer and Reliability Societies, pp. 80-82, March/April 2013.

[12]. Ryan Shea, Jiangchuan Liu, “Performance of Virtual Machines Under Networked Denial of Service Attacks: Experiments and Analysis”, IEEE Journal on Systems, Vol. 7, No. 2, pp. 335-345, June 2013.

[13]. Jerome Francois, Issam Aib, Raouf Boutaba, “*FireCol*: A CollaborativeProtection Network for the Detection of Flooding DDoS Attacks”, IEEE/ACM Transactions On Networking, Vol. 20, No. 6, pp. 1828-1841, December 2012.