ISSN (Online): 2455-7838
SJIF Impact Factor : 6.093

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 4, Issue:5, May 2019

Published By
EPRA Publishing

SJIF Impact Factor: 6.093 Volume: 4 | Issue: 5 | May| 2019 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Peer Reviewed Journal

SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING

Nanda MB[1]
[1] *Assistant Professor Department of computer Science,Sapthagiri college of Engineering,Karnataka,India*

Ramya R[2]
[2]*Student,Dept of Computer Science and Engineering,Sapthagiri college of Engineering,Karnataka,India*

ABSTRACT
An exponential growth of cloud computing is dramatically changing contemporary network service manners. A large scope of cloud-based service offerings, X-as-a Service (XaaS), is empowering flexible adoptions with on demand provisions. However, cloud computing also introduces a series of security concerns, even though there are numerous advantages of using cloud computing. Understanding security concerns in cloud computing is a fundamental requirement for successfully adopting cloud solutions. This paper focuses on a variety of security issues in cloud computing and accomplishes a survey that addresses three major security dimensions of cloud security, including computer security, network security, and information security. Literature review provides a holistic view of cloud security as well as converges recent achievements in the field. The main findings of this work can provide future research in the field of cloud security with theoretical supports and evidence.
KEY WORDS: *Cloud computing, security, privacy,cloud security*

1.INTRODUCTION

With the rapid development of the network technology, cloud computing has bas grown as a broadly accepted deployment in business and has been driving people's lives towards a connected environment. One of the major advantages of cloud computing is that it can offer numerous service models depending on users' demands. Service models can be represented as an X-as-a-Service (XaaS), in which X refers to the computing offerings. Basic computing offerings include infrastructure software, and platform. Meanwhile, service offerings, Xs, can be represented in any manners that are deliverable to users, such as information, security, back-end and process. The flexible service deliveries have remarkably scaled up the service content on the network.

Despite the high convenience and flexibility brought by cloud computing, the implementation of cloud-based solutions is still encountering restrictions deriving from security concerns. Due to the connected environment, cloud computing implementations are facing all vulnerabilities of the network. Meanwhile, besides networking vulnerabilities, cloud applications also need to deal with potential threats from involvers in the cloud, such as unknown third party service providers or unexpected data users. It implies that most cloud applications are facing threats from both insiders and outsiders. Typical cloud risks cover data abuse, malicious insiders, insecure interface and APIs, shared technology issues, data loss or leakage, account or service hijacking, and unknown risk profile. A proper and accurate understanding on cloud security is

a fundamental requirement for a success of the cloud deployment.

This paper thereby focuses on discerning typical aspects of the cloud security. In order to provide a panoramic view of cloud security, we show a high structure of security dimensions in cloud computing. There are three main dimensions, as shown in the figure, which include computer security, network security, and information security. These three dimensions will guide the structure of this survey. At each dimension, the survey only selects significant and representative aspects for reviews due to the limit of pages.

The objective of this work is to provide scholars and practitioners with a knowledge scaffold about recent .The main contributions of this survey are threefold:

(1) This work highlights vital vulnerabilities of cloud security and covers key issues in the field;

(2) We synthesize characteristic solutions to each type of threats in cloud security.

(3) Discussions deriving from main findings provide future security research with theoretical supports.

2. OVERVIEW OF SURVEY PAPERS

2.1 Overview of the survey papers

2.1.1 Real time detection of denial-of-service attack

N lyamin, A.Vinel, M. Jonsonn 2014

Lyamin et al proposed a real time method for detecting DoS attacks in Vehicular ad-Hoc Networks. This method focused on detecting jamming attacks based on the observations of the false alarm probabilities. Another study had an attempt to utilize the advantage of Software Defined Network (SDN) to defeat Distributed Denial-of-service (DDoS) attacks. The authors also highlighted the contradictory relationship between SDN and DDoS attacks such that a few research were raised. Real-time detection of DoS attacks in IEEE 802.11 networks have been studied in , where the proposed detector observes the events happening in the wireless channel and probabilistically computes how ”explainable” occurring of each particular collision is. The method in targets the basic mode of IEEE 802.11 with an arbitrary unicast traffic, which is retransmitted according to the binary exponential backoff algorithm. The method to detect the jammers in VANETs with unicast traffic, which is based on linear regression, is proposed in. However, very limited performance evaluation results are reported in, e.g. no results on the detection time are given. In comparison to the above studies, we consider the beacons, which are transmitted regularly in IEEE 802.11p broadcast mode without retransmissions, making it possible to propose an alternative jamming detector. To the best of our knowledge no literature has considered the problem of jamming DoS attacks detection in VANET platoons so far.

Limitations

Probability of detection is of low range.

Too much of assumptions in the presented model especially in beaconing period.

2.1.2 Analysis of clickjacking attacks and an effective defense scheme for android device

L.Wu,B.Brant,X.Du and B.Ji 2016

Wu et al emphasized that a stealthy clickjacking attack could take place by clicking on any malicious object on the page, such as a fake system reminder. Users would not notice the adversial activities since re-launching malicious software could be automatic, such as using a timer. We systematically study mobile clickjacking attacks from the perspective of floating window and target window, separately. We discover and analyze more unique features of clickjacking including the window flags, transparency, etc., which make our detection scheme more accurate than existing solutions which mistakenly accuse some benign apps due to their coarse policies. We investigate the “after-attack” disguises to keep the clickjacking undiscovered after one successful attack, which has not been considered in previous works. Specifically, we present three types of side-channels that allow the malicious app to listen to the user input events. We explore a variety of clickjacking attacks, targeted on system apps, 3rd-party apps, and other particular system UI. The threat of clickjacking is better evaluated than previous works which only have a couple of examples for illustration. Our detection scheme outperforms previous methods as it requires no user/developer involvement and is compatible with Android system design as well as existing apps. We implement the proposed scheme on real smartphone. The experimental results show that it is effective and efficient**.**

Limitations

There is an impact to the system performance. During the hierarchy change of window,hierarchy is still performed

2.1.3 VeriTrust: Verification for hardware trustJ.

Zhang,F.Yuan, L.Wei,Y.Liu 2015

Tsoutsos et al developed an zero-overhead privilege escalation approach for microprocessor modifications. Another study explored an approach using multi-IDS systems that could detect privilege escalation or backdoor attacks in multi-tier web applications. Additionally, Zhang et al argued that it was possible to prevent backdoor attacks at the system design stage by using their proposed technique. The approach was called VeriTrust that continuously examined verification corners for identifying potential adversial triggers.We classify HTs into two categories, bug-based HTs and parasitebased HTs, based on their impacts on the normal functionalities of the circuit, and discuss their corresponding characteristics. We present the so-called VeriTrust technique to detect parasitebased HTs

by identifying the dedicated trigger inputs used in HTs. Unlike existing HT detection algorithms, VeriTrust is insensitive to the implementation style of HTs and hence prevents attackers from defeating it by simple HT modifications.We propose several techniques to reduce the memory usage and runtime of VeriTrust to make it scalable to large circuits.

Limitations

- Attackers may exploit the assumptions used in VeriTrust to evade it.
- Verification test cases may miss identifying the malicious behavior of HTs.
- Time complexity and ineffective cost.

2.1.4 A hierarchial attribute based solution for flexible and scalable access control in cloud computing

Z.Wan,J.Liu and R.Deng 2012

Liu et al had a focus of data security in the financial industry and proposed an attribute-based semantic access control method. This method used ontologies to formulate relationship between data owners and data usage to avoid unexpected parties reaching data in the context of cloud computing. Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt et al. and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

Limitations

- Data consumers are allowed to access for reading purposre only.
- Neither data consumers nor data owners will be online always.

2.1.5 Multiattribute SCADA-Specific Intrusion Detection System for Power Networks

Y Yang, K.McLaughlin,S.sezer,T.Littler 2014

Yang et al points out that ARP's vulnerability that it does not have a verification mechanism for verifying authenticity of the ARP messages, even though it is a trusting protocol. Attacks often take place from malicious hosts in an LAN. The increased interconnectivity and complexity of supervisory control and data acquisition (SCADA) systems in power system networks has exposed the systems to a multitude of potential vulnerabilities. In this paper, we present a novel approach for a next-generation SCADA-specific intrusion detection system (IDS). The proposed system analyzes multiple attributes in order to provide a comprehensive solution that is able to mitigate varied cyberattack threats. The multiattribute IDS comprises a heterogeneous white list and behavior-based concept in order to make SCADA cybersystems more secure. This paper also proposes a multilayer cyber-security framework based on IDS for protecting SCADA cybersecurity in smart grids without compromising the availability of normal data. In addition, this paper presents a SCADA-specific cybersecurity testbed to investigate simulated attacks, which has been used in this paper to validate the proposed approach.

Limitations

- a large number of viable cyber security issues exist against smart-grid SCADA systems, which could threaten digital substations.
- a significant challenge in this area of research is the lack of an openly available test dataset to compare the performance and accuracy of proposed solutions.

3.1 SECURITY DIMENSIONS IN CLOUD COMPUTING

3.1.1 COMPUTER SECURITY

Computer security is a wide concept that covers most aspects of computer system protections. The protection objectives include hardware, software and information. This section selects three typical aspects of computer security, which are attack types, access control, and cryptography.

1.Attack Types: We summarize a number of typical attack types in this section, which include Denial-of-Service (DoS), click jacking, eavesdropping, spoofing, social engineering, tampering, privilege escalation, and backdoor attacks. Each attack is specific or non-specific to th networking connection layer or operating system. Fig. 1.2 shows a synthesis of the typical attacks and their attached layers. A brief review about attack types is given below.

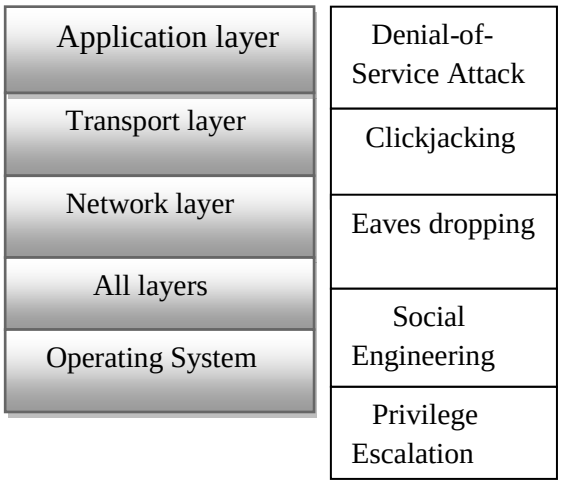

Fig 1 Main attack types and their layers

First, a DoS attack is a group of malicious methods that prevent users from reaching the desired computing resource via the network. Main issues have been surveyed by prior work that can be referred to literatures . Next, a Click jacking attack generally is considered an adversarial activity at the transport layer. The attack usually is attached to a browser, in which the attack is launched by a clickable object on the page with embedded adversarial codes or a script. Some examples of click jacking included Like jacking and Cursor jacking.

Furthermore, eavesdropping and spoofing are two attack methods that generally take place at network layer. An eavesdropping attack mainly targets at those unencrypted data by capturing small packets for stealing information. A spoofing attack is an adversarial action that pretends to be a legal communicator by making fake data or identity. Recently, some studies have tried to lower down the chance of eavesdropping attacks. For instance, an investigation has attempted to examine whether a dynamic encryption strategy could increase privacy protection. This method gave those data that carried sensitive information the priority in order to deal with the computation workload caused by big volume data. From the perspective of adversaries, a research proposed a mixed method that combined spoofing and jamming attacks. The attack effect could be maximized when considering the restriction of the power supply.

Moreover, some attacks may take place at all layers, such as social engineering and tampering attacks. A social engineering attack is a type of adversarial actions utilizing psychological behaviors for the purpose of information stealing. Some examples of social engineering techniques are Pretexting, Phishing, and Baiting attacks. A tampering attack is a presentation of a group of attacks that modify software settings or hardware configuration without users' permissions.

Finally, privilege escalation and backdoor attacks are two common malicious actions at the operating system layer. A privilege escalation attack mainly describes an adversary who utilizes vulnerabilities/bugs of the system to obtain the access to the information. A backdoor attack refers to adversaries learn the hidden part of the program or system and utilize it to illegally obtain information.

2.) Access Control

An access control system refers to a series of system configuration that determines whether a user can have the access to a certain information. The mechanism of an access control system is to examine whether the access requester matches the criterion. Common network access enforcement methods include IEEE 802.1X, Virtual Local Area Networks (VLANs), firewall, and Dynamic Host Configuration Protocol (DHCP) management. Meanwhile, the core of most access control systems is applying a Computer File System (CFS), which creates a list of requirements/criterion for access examinations. A main vulnerability of contemporary CFS is that the system may be fooled by adversaries by making fake data for matching criterion. In line with current access control settings, there are a few components in a typical access control system. Four main parts are shown in Figure. Among these components, authentication methods are usually concerned by system designers. Applying an Extensible Authentication Protocol (EAP) transport service can support the authentication information exchange between client system and an authentication server. Some examples supported by EAP are EAP Transport Layer Security, EAP Tunneled TLS, EAP Generalized Pre-Shared Key, and EAP-IKEv2.

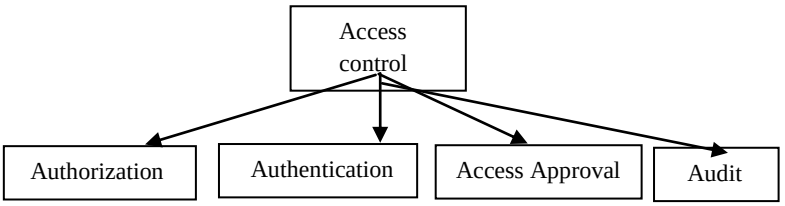

Fig. 2 Main components of access control.

Moreover, some advanced access control approaches have been explored by recent research as well. One popular research direction is to design an Attribute-based Access Control (AAC) to strengthen the security. The advantage of using an AAC method is that some attributes can be hardly fabricated by adversaries.

3.Cryptography in Clouds

Cryptography in cloud computing has its own characteristics. An ideal cryptographic design for cloud-based applications need to deal with both insider and outsider threats. However, most cryptographic approaches could only take care one side, mostly outsider threats. In fact, threats from

insiders also restricts the implementation of cloud solutions, due to uncertain operations done on the clouds and unknown parties who have accesses to the data.

There are three advanced encryption types that match the requirement of cloud computing for both insider and outsider threats. The first option is an Attribute-based Encryption (ABE). This type of solutions has been explored over years and two common kinds of ABE are Cipher text policy ABE (CP-ABE) and Key-policy ABE (KP-ABE).Moreover, the second alternative is Fully Homomorphic Encryption (FHE). A proper FHE allows arithmetic operations over the decrypted data in the cloud, such that cloud operators (insider threats) cannot access plain-texts. The implementation of FHE can be also combined with other security protocol to against threats from outsider. A basic manipulation process of an FEH is shown in Fig1.4. We can observe that operators on the cloud sider always reach encrypted data.

Despite a perfect match for cloud computing, there is no active FHE adoption in practice. Gentry's FHE is considered the first logical method for achieving homomorphism encryptions. However, this approach is far away from the practical implementation due to its heavy computations and noise creations. Many scholars have tried to improve the efficiency of this approach from both cryptographic design and hardware, but current performance still cannot satisfy the requirement of the industry.

Recent break-through of FHE design took place when a totally distinct direction was addressed. A new design was proposed, which used tensor theory to achieve homomorphism results. The advantages of this approach are threefold. First, the complexity of this approach was lower than Gentry's method so that its execution efficiency was higher. Second, this approach did not create noise during the whole mathematical process; thereby, data users can always obtain accurate results. Finally, data can be secured during the whole process of data usage. The problem of this approach is that the workload of decryptions is heavy.

Finally, the last option for cloud-oriented encryption is Searchable Encryption (SE) that can be referred to literatures . This type of encryptions emphasizes the searching operation rather than mathematic operations. The main challenge of this type of encryption is that it generally requires a large of key distributions for both encryptions and searching. Naveed et al. highlighted the problem of identifying basic primitives to achieve blind storage. Another study also addressed the problem of the key distributions and designed a concept of key aggregate searchable encryption. In this approach, only one single key is required by a data owner for sharing sharing a large amount documents with one user.

3.1.2 NETWORK SECURITY

Here we discuss about the main issues in network security, which are attack types and recent explorations in enhancing security of the network.

1. Attack Types

The attack types in network security have many overlaps with computer security. As a web-based technique, cloud computing is facing all network-oriented attack types. From the perspective of the attack triggers, types of attacks can be categorized into two groups, namely, passive and active attacks.

A passive attack refers to malicious activities that grabs information while directly intercepting traffics of the network. Common methods against passive attacks include wiretapping, port scanner, idle scan, data encryption, and traffic analysis. Meanwhile, an active attack means that an intruder who distorts networking operations or obtains access illegally via malicious codes. A few typical active attacks include virus, eavesdropping, DoS attack, spoofing, Smurf attack, man in the middle attack, ARP poisoning, buffer overflow, heap overflow, SQL injection, phishing, and cross-site scripting.

First, Address Resolution Protocol (ARP) poisoning is a kind of active attack that relies on the spoofing attacks on a Local Area Network (LAN) via a spoofed ARP message. Basic idea of ARP poisoning is causing traffic deceiving via pretending a host's IP address so that LAN users send message to malicious users instead of the default gateway

Next, a Smurf attack is a kind of DDoS attack that launches a traffic flood to the victim's device over the Internet Control Message Protocol (ICMP). The process of theSmurf attack mainly consists of two steps. The first step is that an attacker send out ICMP packets with spoofed IP to numerous devices. The second step is that the attacker receive ICMP responses and redirect them to the victim device. Thus, victim device will receive a flood traffic if the number of the responses is great. We provide a process diagram of Smurf attack in Figure

2 . Network Security Enhancement

As one of the most broadly adopted security services, Secure Socket Layer (SSL) establishes an encrypted connections between a web server and a browser. Its implementations are generally based on a set of security protocols. With the development of the Internet, SSL cannot satisfy the requirement of the security and is being replaced by another protocol set that is Transport Layer Security (TLS).

Moreover, the methods against adversaries are various and some of them are mentioned in prior sections. Each defense method may be suitable for one or multiple network threats. Representative defense methods include access control, software-oriented security tool, authentication, authorization, cryptography, firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and secure

gateway. A passive attack refers to malicious activities that grabs information while directly intercepting traffics of the network. Common methods against passive attacks include wiretapping, port scanner, idle scan, data encryption, and traffic analysis.

3.1.3 INFORMATION SECURITY:

This section concentrates on the information security issues in cloud computing. Two aspects are involved in this security, which are identity management and privacy protection.

1. Identity Management:

The concept of identity management is a group of activities to verify whether a person or a group of users has/have access to a computing object, such as an application or a system. Major activities during the verification process include identification, authentication, and authorization. It has an overlap with the operation of the access control. However, identity management and access control have distinct focuses. Normally, identity management focus on authentication, while access control mainly addresses authorization. Moreover, there are some challenges for current identity management from the perspective of the implementation. The first challenge is password management in a distributed environment. The cost of identity management will be increased when authentication systems are deployed in multi-geographic locations. The other challenging issue is to secure identity information. In the distributed context, attackers have a chance to monitor identity information if authentication system is connected to a remote server. There will be more threats when wireless networks are used.

1.)Privacy Protection:

Privacy concern is a common issue in the implementation of cloud computing. Data carrying sensitive information are adversaries' targets. What is more, data owners have rare control on their data when data are stored/operated on the remote cloud server. Data trades between service providers also threaten users' privacy.

A few approaches can enhance the level of privacy protection in the cloud. First, increasing data control during the whole data usage cycle can reduce the risk caused by loss of control. A data usage cycle covers a chain of states, including at rest, in transit, in use, and access. Next, encryption is a positive alternative for data owners (clients) to prevent data from malicious actions during transmissions. In most situations, an encrypted data package is assumed to be secure. Future solutions may include advanced encryption technique, such as FHE and block-chain techniques. Finally, a multi-encryption strategy will become a trend to deal with big data privacy. Encryption priority will be given to those data that carry sensitive information so that the selection of the encryption is a dynamic work

3. CONCLUSIONS

In this paper,a survey was accomplished to review all crucial security aspects of cloud computing. The convergence was organized by three parts, which were computer security, network security, and information security. The literature review synthesized major threats and vulnerabilities of cloud computing, as well as the corresponding defense methods or potential solutions. The survey also depicted that security issues in cloud computing derived from both insider and outsider threats. Traditional security protocols could mainly prevent risks from outsider threats; an effective FHE was a desired solution even though there was yet no ubiquitous solution available.

FUTURE WORK

With the development of the Internet, SSL cannot satisfy the requirement of the security and is being replaced by another protocol set that is Transport Layer Security (TLS).This layer has to enhanced in a better way. Common methods against passive attacks include wiretapping, port scanner, idle scan, data encryption, and traffic analysis.

REFERENCES

1. *N. Lyamin, A. Vinel, M. Jonsson, and J. Loo. Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. IEEE Communications letters, 18(1):110–113, 2014.*
2. *L. Wu, B. Brandt, X. Du, and B. Ji. Analysis of clickjacking attacks and an effective defense scheme for android devices. In Communications and Network Security (CNS), 2016 IEEE Conference on, pages, Philadelphia, PA, USA, 2016. IEEE.*
3. *Z. Wan, J. Liu, and R. Deng. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE transactions on information forensics and security, 7(2):743– 754, 2012.*
4. *N. Tsoutsos and M. Maniatakos. Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation. IEEE Transactions on Emerging Topics in Computing, 2(1):81–93, 2014.*
5. *Y.Yang, K.Mc Laughlin, S.Sezer, T.Littler,E.Im, B.Pranggono, and H. Wan Multiattribute scada-specific intrusion detection system for power networks. IEEE Transactions on Power Delivery, 29(3):1092–1102, 2014.*