Cloud Security and REST APIs Developing in Web Application

Himanshu Singh
Galgotias University
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Anuj Sahu
Galgotias University
2 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Cloud Security and REST APIs Developing in Web Application

Department of Computer Science and Engineering
Galgotias University
Plot No 2, Sector – 17 A, Yamuna Expressway,
Greater Noida, Gautam Buddha Nagar, UP, India

Himanshu Singh
B. tech (CSE)
Galgotias University
Greater Noida, India

Anuj Sahu
B.tech (CSE)
Galgotias University
Greater Noida, India

Harsh Vardhan Pathak
B.tech (CSE)
Galgotias University
Greater Noida, India

Submitted To
Ms. Mudita Sharan
Assistant Professor
School of Computing Science and Engineering,
Galgotias University Greater Noida, India

GALGOTIAS UNIVERSITY
(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

School of Computing Science and Engineering,
Galgotias University Greater Noida, India

Abstract—

Most modern cloud and web services use REST APIs. This article describes how an attacker can exploit a REST API vulnerability to gain access to services. We introduce four new security policies using REST APIs, then show how to extend the REST API fuzzer with a device inspector that tests and identifies violations of these rights. We will consider how and how much to use checkers modularly in two ways. Using this tool, we find many new bugs in production Azure and Office365 cloud services, discuss their security implications, and cover them all.E-commerce is a purchase and sale of goods and businesses, or transfer of property or information through an electronic network, basically the Internet. These trade exchanges happen either as b to b (business to business), b to c (businesses and consumers), c to c(consumer-to-consumer) or c to b (consumer-to-business) This is an exchange of items or services using computer networks such as the Internet or online informal communities. He did business here using computers, telephones, faxes, barcodes readers, credit cards, ATMs or other electronic appliances without replacing paper ones documents or physically move to the mall. It includes activities such as purchase, contract entry, exchange processing, online payment, authentication, inventory control, order fulfilment shipment and customer support. When the buyer pays with a bank card swiped through a magnetic stripe reader, he is interested in e-commerce. Cloud computing provides on-demand services over the Internet with the help of large amounts of virtual storage. The main feature of cloud computing is that the user does not have to set up expensive computing infrastructure and its costs there are fewer services. In recent years, cloud computing has been integrating with industry and many other fields, which is encouraging researcher to research new related technologies. Due to the availability of its services and scalability for computing processes individual users and organizations transfer their applications, data and services to a cloud storage server.

Keywords— *Cloud Computing, Cloud Framework, Cloud Security, Cloud Security Challenges, Cloud Security Issues, e-Commerce, Security, Threats and Vulnerabilities, Firewall, Session Hijack, Viruses.*

1. INTRODUCTION

The use of cloud computing is explosive. Over the past few years, cloud service providers such as Amazon Web Services [2] and Microsoft Azure [13] and their customers who have "digitally improved" their businesses have delivered thousands of cloud services. written. and identify various new information.Security in electronic commerce is part of the information security framework and is specifically applied to the components that affect e-commerce that involve the computer Security, data security. E-commerce needs high security components that influence end user through their daily payment interaction with the business. Eshop required a reliable infrastructure and framework to enable secure and successful e-commerce. Protection and security are a remarkable concern for electronics today technologies such as M-commerce (Mobile – Commerce) share security concerns with others and e-commerce associations. On the web, e-commerce applications that process payments, such as saving money online, electronic exchange or use of debit cards, credit cards, PayPal, electronic money, prepaid cards, major cards, visa cards or other tokens have more compliance, technology issues in the field. Concerns about protection have been discovered, revealing an absence of trust in a variety of contexts, including business, electronic health records, electronic recruitment technology and long-distance interpersonal communication, directly affected users.

In this work, we present four security methods for REST APIs and services to get good results.

After free use policy: Deleted files should no longer be used.

Legal Leak: Incompletely created resources should not be accessed and side effects of backend service state should not be "discovered".

Resource Hierarchy Rule: Child resources of a parent cannot be accessed by other parent resources.

Username Policy: Resources created under the username cannot be accessed by other usernames.

Security is one of the most important variables that limit customers and associations involvement in e-commerce and e-commerce is currently being addressed gradually for security issues on their internal networks. There are such instructions for security of systems and networks available to e-commerce systems personnel read and implement. As a large part of customers use these services online shopping some are literate and some are illiterate thus educating consumers security issues are still at an early stage. Nevertheless, it turns out that the most a fundamental element of e-commerce security architecture.

Historically, a computer would take up as much space as a a room with extravagant electronic components such as network devices, processor to generate less output processing, demanding so much performance compared to modern computers. Nowadays, these sufficient spaces are replaced by small hard ones replaces drives and expensive electronic parts with economical ones network devices. This increase in computing power a infrastructure nodes can be the source of a large distributed system

which brings together a large number of resources in the unit it supports
highly exhaustive calculations such as scientific simulations.
Two well-known components for a distributed system are clusters and lattices [151]. Clusters and grids are both different approaches. The cluster model supports linkage homogeneous networks, while grids are designed for large distributed and heterogeneous networks. Cluster the model is more expensive due to expensive central processing
units such as parallel supercomputers. Separate resources of desktop computers is connected by middleware
like MPICH and is a cheaper approach. The grid is the most
commonly used desktop and home user architecture for creating service computing nodes and is created via internet. Large Hadron Collider (LHC) calculation.
the CERN grid is a good example of such a network. Main the disadvantage of grid computing is its increased management
and task of complexity and create interference at result collection time.
We define tools to measure weather forecast through RE ST APIs and test objects.

Check if the service is reliable.We also check for bugs a nd fix them using the REST API.

2. LITERATURE REVIEW

In general, interpersonal trust focuses on the extraordinary contingency that we usually discuss business, for example the customer's trust in the seller. Rada et al
that consumer trust can have multiple referents such as item, seller, and friends
and as appropriate to define trust as a worldwide belief towards the buyer that
seller, item and friends will satisfy their obligations as they understand them
buyer. Likewise, in the context of e-commerce, some as researchers have tended to
define and describe trust as a person's willingness to be vulnerable, a person's willingness
expectations and subjective beliefs, reliance on parties other than oneself or a
subjective probability.
On one hand, e-commerce website owners are considering how to engage more
customers and how to make guests feel safe when they break away on site,
while on the other hand, how should end users evaluate e-commerce websites and
what should they do to protect themselves as one of the online networks (V.
Srikanth (2012)). Every stage of an e-commerce exchange has security measures.
Viruses are a vexing threat in the world of e-commerce. They only disrupt e-commerce operations and should be classified as Denial of Service (DoS) device. Password protection, encrypted client-server correspondence, open
private key encryption schemes are completely negated by the simple fact that
the trojan horse program allows the hacker to see all the plain text before they get to it
encrypted (Randy C. Marchany, Joseph G. Tront, (2002)). Due to the increase in
admonishing the media against security and safety breaches such as identity theft
and misrepresentation of money-related information and increased awareness of online
customers about the threats of making exchanges online, e-commerce does not
managed to reach maximum capacity. Many customers refuse to make online exchanges and relate to it
absence of trust or fear of their personal data (Rashad Yazdanifard, Noor Al-Huda
Edres, (2011)). Obviously, an online exchange requires consumers to disclose a large amount
measuring sensitive personal data for sellers, putting them in a critical state
danger. Understanding (and even precisely defining) consumer trust is essential
for the development of e-commerce (Pradnya B. Rane, Dr.
B.B. Meshram, (2012)). Some of the researchers analyzed the technologies in
Transaction security for an e-commerce application as an encryption approach:
Encryption is the process of converting plaintext or information into ciphertext
cannot be read by anyone other than the sender and recipient. Purpose
encryption is: (1) security of stored data and (2) security of data transmission (Chaum,
David. 1985). Secure Socket Layer: The most well-known type of security channels is
via SSL (Secure Sockets Layer) TCP/IP protocol. The SSL convention provides
information encryption, server authentication, voluntary client authentication,
and message integrity for TCP/IP connections. Secure Socket Layer (SSL) is a
security convention first developed by Netscape Communications Corporation and
now taken over by vehicle layer security work assemblies.
The design goal of the convention is to prevent eavesdropping, unauthorized manipulation or
message forgery when information is transmitted over the Internet between two
transport application (Pradnya B. Rane, Dr. B. B. Meshram, 2012), Safe
Hypertext Transfer Protocol (S-HTTP): S-HTTP is a secure, message-oriented protocol
interchanges convention designed for use in conjunction with HTTP. It is designed to
coexist with HTTP and be easily integrated with HTTP applications. While SSL
is designed to establish a secure connection between two computers, S-HTTP is

designed for secure sending of individual messages. Any message can be using S-HTTP
be signed, authenticated, encrypted, or a combination thereof. In general, S-HTTP
attempts to make HTTP more secure (Shazia Yasin, Khalid Haseeb, 2012), digital
Signature: Computer signature means an advanced method performed by a
collection with the intention of verifying a record that is unique to that individual
uses it and is capable of verification. It is associated with information in such
way, to the extent that if the information changes, the electronic signature does
invalidated. A guaranteed signature is usually a hash of a message that is
encrypted with the owner's private key (Delaigle, J-F., C. De Vleeschouwer, and B.
Macq. 1996).
Secure Electronic Transaction (SET): The SET specification for a credit/payment card
exchange is necessary for the safety of all involved in electronic commerce. It is designed to
to fulfill three basic objectives. First of all, it will enable payment security
for all involved, verify cardholders and merchants, ensure confidentiality for
payment information and define conventions and potential electronic security
service providers. It will also enable interoperability between applications
developed by different vendors and between different operating systems and stages
(Anderson, Ross. 1994), Digital Certificate: An Advanced Certificate is Computerized
a document issued by a trusted external entity known as a certification
specialist that contains the name of the subject or organization, the subject is open
key, advanced certificate serial number, expiration date, issue date,
computer signature of the certification expert and other identification data. The
A Certificate Authority (CA) is a trusted outsider that issues certificates and
publishes identities and public keys in the directory. The certificate is signed with
the certificate authority's private key; so its authenticity can be confirmed
using a known CA public key.

3. METHODOLOGY

A. Stateful Rest API Fuzzing

In our opinion, the REST API is the best way to reach th e cloud by providing security. Requesters submit request s for services and receive responses based on service res ponses. A secure protocol called HTTP/S is used to carr y this type of communication. When receiving a respons e, it connects to the HTTP event state, which is 2xx, 3xx, 4xx or 5xx.
Swagger is a descriptive language called OpenAPI for d escribing REST APIs. For RESTful services, Swagger s pecifies which requests can be made and what types of r esponses can be returned. The response type is also speci fied.

The request is interpreted as part of the REST API. To m eet users' needs, each request has the following four para meters <a,< span="" style="margin: 0px; padding: 0px;">t, p, b> where
is the authentication type
a, the mode request
t, the route
p, and the request body
b. .
</a,<>B. Security Checkers for Rest APIs

We provide four security checks for REST APIs and ser vices to capture the features they need. All four rules are based on real bugs discovered through manual penetrati on testing or root cause analysis of customer issues in cl oud services in the past. New issues discovered due to br eaches in production Azure and Office 365 services will be discussed and bugs fixed.

We use the code with the help of the testers.
The main driver for stateful REST APIs to discover the s tateful environment, active controllers provide additional checks to ensure that certain rules are not violated. For t his reason, researchers often expand the search space by conducting additional tests designed to break certain rule s.

We create active controllers using a standard model that adheres to the following two principles:

The controller is not dependent on the main promoter for REST API blurring, and their presence has no effect on the latter's call state.
Controls do not interfere with any method, they are teste d by checking requests made by the main driver and ign oring requests made by other controllers.
Post-Free Checker
Resource Leak Checker
Resource Hierarchy Checker
User-namespace Checker
Combining all these checkers with the REST API Fuzzer to generate code.
Stateful REST API fuzzing is extended by the tester to

Expanding the state space by running additional tests, lo oking for answers other than
5xx, which may be indicative of a criminal problem. The refore, the use of the controller can increase the driver's knowledge of the disease.

4. CLOUD COMPUTING ARCHITECTURAL FRAMEWORK

In this section, the basic cloud computing architectural framework is presented, shown in Fig. 1. To understand the security issues, first it is important to understand the basic concept and framework of cloud computing. The NIST defines three service delivery models, five essential characteristics, and four deployment models, that is widely accepted [113].

4.1Essential characteristics

There are many characteristics of cloud computing, but here we focus on five main characteristics, provided by the NIST [113]:

On-demand self service

It enables consumers directly request, manage and access services through the website services and management interfaces without human interaction.

Wide network access

Data and services are presented in the cloud must be accessible using any standard devices such as mobile phones, PCs, desktops, laptops. These devices work through some standard protocols and technologies. The nature of cloud computing should support all standards protocols.

Resource Pooling

The cloud provider provides a large physical or virtual computing resources that are shared with each other more users. These resources are allocated dynamically multi-tenant environment.

Rapid elasticity

Elasticity is a key feature of the cloud. The resource usage of this property is scaled according to consumer demand. Customers have unlimited resources which can be purchased as needed on a pay-as-you-go basis.

Metered service

According to user demand and payment automatically serve the meter of the cloud system control and scale resources.

4.2 Service models

The service model provides a list of services; these are provided by the service provider and consumed by the consumer. Software as a Service SaaS provides a standard Integrated Development Environment (IDE) to your client access applications and transfer data and applications to remote storage server through online software services. Salesforce.com and Customer Relationship Management (CRM) are such an example that fulfills the SaaS model.

Infrastructure as a service IaaS refers to virtualized resources offered by a cloud service provider in the form on demand, including compute, storage, network, memory, processor and communication. Amazon Web Service [10] (AWS) is the best example of IaaS that gives EC2 services as a virtual machine with a software stack.

Platform as a Service Platform-oriented cloud provides higher level programmable platform, known as Platform as a Service. It provides an easily programmable cloud platform the multiple programming models, IDEs, specialized services, operating systems, and platform-level resources that are used created, run, deployed and managed by cloud consumers their applications. Google App Engine is the best example of this.A Platform as a Service that provides an extensible environment in which developers develop and host web applications.

4.3 Deployment models

The cloud computing deployment model is about types cloud.

Private cloud A private cloud is operated and maintained internally by a single organization or through a third party Auditing (TPA).

Public cloud The public cloud is operated and managed by the company CSP and physical infrastructure can be presented off-site user location. Cloud resources are shared between more people and people pay cloud providers accordingly on the services they use.

Community Cloud A cloud that is deployed and shared between a group of people to share a common interest, such as mission, security policy, applications and services are known as community cloud.

Hybrid cloud A hybrid cloud is a mixture of two or more clouds with the same infrastructure and capabilities.

4.4 Storage models

The storage model tells how to store data in the cloud and storage space availability. The cloud environment provides many types of storage solutions. Each solution has its own benefits and limitations, based on demand and available data consumer to choose a suitable storage system [91].

Shared file/block storage system A file consists of the number of data located in folders that are shared between multiple users/hosts using the Internet. More users access files through standard protocols or options. They it can use any of the protocols such as Network File System (NFS), Server Message Block (SMB) and Common Internet A file system (CIFS) for storing and accessing data.

Object Storage System In an object storage system, data are stored/accessed in the form of objects. Every subject is accessible by global key, hash, or Uniform Resource Locator (URL) using Representational State Transfer (REST) or the web cloud services based on services using the Hypertext Transfer Protocol (HTTP) as primary protocols. Cloud data management interface (CDMI) provides an interface to store objects for access objects.

A database or tabular storage system Many industries store their data in the form of a Relational Database or a Relational Database Management System (RDBMs), so they are stored in the row and column shape. We are in a relational database maintain data integrity and avoid data redundancy. Scale and performance are major issues in cloud sessions database.

4.5 Cloud role and boundaries

The cloud provides different types of predefined roles organization and person. It is described in the following subsection the roles and responsibilities of each participant and how they interact with the cloud.

Cloud Provider Cloud Provider refers to an individual or an organization that implements/provides cloud resources. The the primary responsibility of a cloud provider is to create a provide cloud services to cloud users according to the SLA guarantees.

Cloud Consumer A cloud consumer is a person or human an organization that consumes company-provided cloud IT resources cloud provider.

Cloud service owner Cloud customer or cloud provider both are identified as the owner of the cloud service. Cloud service owner referred to as the person or organization that legally owns a cloud service.

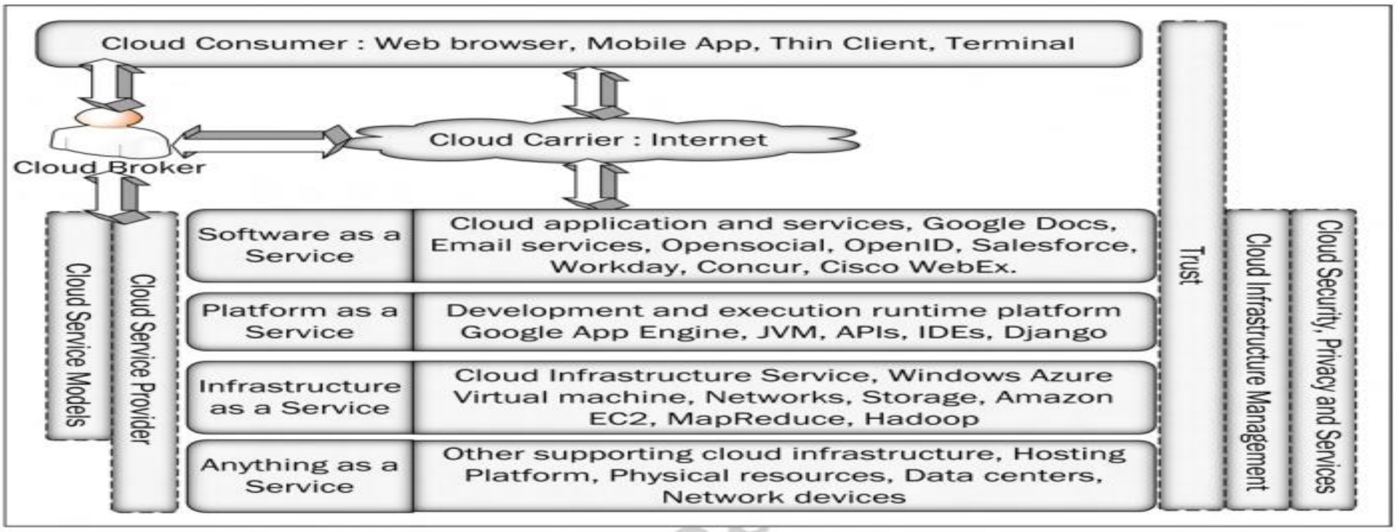
Cloud Resource Manager A person or organization which performs the management task for cloud services, including cloud resources known as cloud resource managers.

Organizational Boundaries Organizational boundaries define the physical boundary that surrounds a cloud set IT resources that are actually owned by the organization. An organizational boundary does not mean a boundary real organization, surround only an organized set of IT resources.

Trust Boundaries When a cloud consumer accesses the cloud IT resources, it must be a need for trust that crosses borders the physical boundary of the organization from which to combine the element cloud environment. A confidence limit is a logical circle which usually cover the entire cloud architecture [23] trusted IT resources.

Other roles The main role of a cloud auditor is to investigate all computing, storage, performance and security threats in the cloud space. Generally, the auditor is a third party authentication entity that provides a secure access environment for all subjects.

Cloud broker is generally an application program or individual that provides an interface between the client and provider. A cloud carrier is a connection, communication link, or the medium between all the entities that the consumer allows access to various services. In general, in the cloud, the Internet is the carrier, the use HTTP protocols for transferring information to all entities.


Cloud Consumer : Web browser, Mobile App, Thin Client, Terminal
Cloud Broker
Cloud Carrier : Internet
Cloud Service Models
Cloud Service Provider
Software as a Service
Cloud application and services, Google Docs, Email services, Opensocial, OpenID, Salesforce, Workday, Concur, Cisco WebEx.
Platform as a Service
Development and execution runtime platform Google App Engine, JVM, APIs, IDEs, Django
Infrastructure as a Service
Cloud Infrastructure Service, Windows Azure Virtual machine, Networks, Storage, Amazon EC2, MapReduce, Hadoop
Anything as a Service
Other supporting cloud infrastructure, Hosting Platform, Physical resources, Data centers, Network devices
Trust
Cloud Infrastructure Management
Cloud Security, Privacy and Services

5 CLOUD TECHNOLOGY

In modern times, the cloud uses a set of technological components that enables the key functions and features of cloud computing. In this section, we define such technologies that help us to do this understand how these technologies are deployed in the cloud infrastructure.

5.1 Broadband network and Internet technology

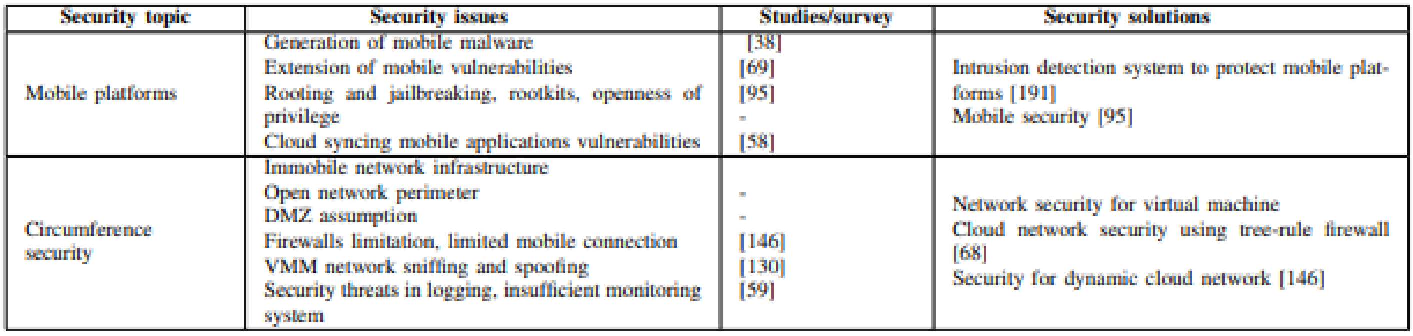
The Internet allows users to access remote cloud IT resources to support ubiquitous network access. This an unavoidable requirement creates a built-in dependency on Internet. The Internet device is set up and deployed by an Internet Service Provider (ISP). Any ISP can freely select, manage, deploy and add another ISP to your networks.

There are two types of connections available on the network technology, one of which is connectionless packet switching (datagram) and another is a router-based connection.

In connectionless packet switching, the sender's data is split into multiple packets (datagram) and each packet follows different paths to reach the destination address. In a router-based connection, the sender's data is divided into several fixed ones packet size, follow the same path to reach the destination address using the router.

5.2 Data center technology

Data center technology includes multiple technologies and components that are usually stacked with each other. The the data center has both physical and virtualized IT resources.



Security topic	Security issues	Studies/survey	Security solutions
Mobile platforms	Generation of mobile malware Extension of mobile vulnerabilities Rooting and jailbreaking, rootkits, openness of privilege Cloud syncing mobile applications vulnerabilities	[38] [69] [95] - [58]	Intrusion detection system to protect mobile platforms [191] Mobile security [95]
Circumference security	Immobile network infrastructure Open network perimeter DMZ assumption Firewalls limitation, limited mobile connection VMM network sniffing and spoofing Security threats in logging, insufficient monitoring system	- - [146] [130] [59]	Network security for virtual machine Cloud network security using tree-rule firewall [68] Security for dynamic cloud network [146]

The physical IT resources including network systems, homes computing, servers and devices, consisting of hardware systems. A virtualized IT resource is placed above virtualization layers that are operated and managed by the virtualization platform. Modularity and standardization are basic requirements to reduce restrictions, traffic and cloud investment costs. The data center is built with using standardized commodity hardware and modular architecture, multiple aggregations, unique building blocks k provide scalable, incremental service growth.

5.3 Virtualization technology

Virtualization is a conversion process that converts physical IT resources into virtual IT resources. IT resources they include servers, storage, network and power. Virtualization the software provides the coordination capacity of the host which enable multiple virtual servers that are connected and communicate with each other in the same host. Virtualization allows virtual servers to create a virtual disk image that contains a virtual server backup file. Virtualization it is created by two types: operating system-based virtualization and hardware virtualization. Based on the operating system virtualization, virtualization software is installed on a pre-existing operating system (host operating system). The the second hardware virtualization is about installation virtualization software directly on the physical host hardware. After installation, it is passed to the host operating system.

5.5 Web technology

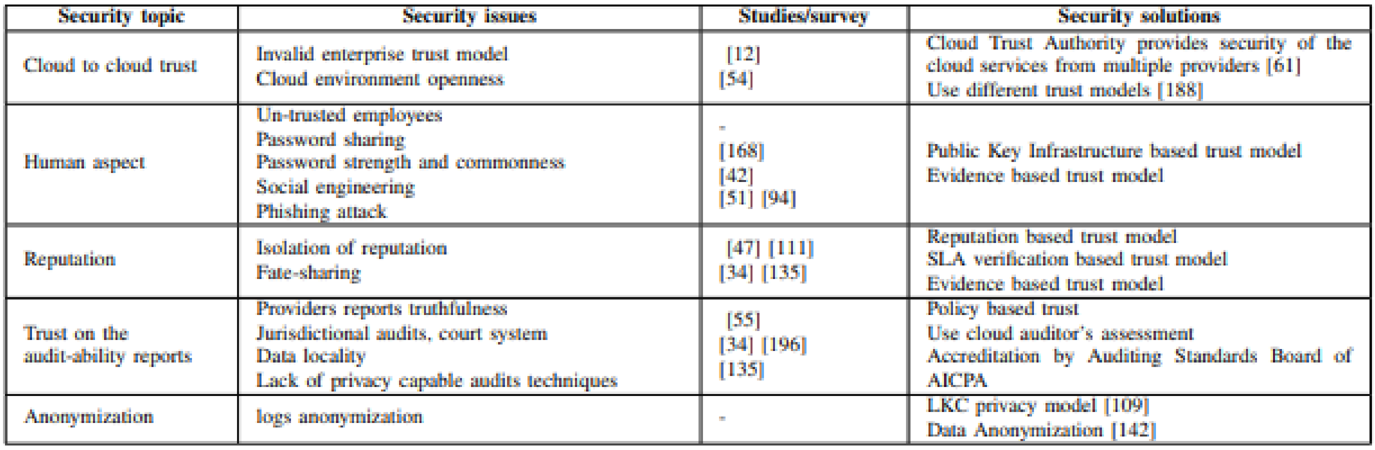
Web technology is an emerging development trend cloud computing. The basic concept of cloud computing is based on the Internet. A web browser, based on the web applications and services are implemented and managed specialized web technologies. World Wide Web (WWW) is an internet technology that is used to connect several IT resources. Two basic components web technology is a web client and a web server. Proxies, routers, cache server and gateways are known as secondary components of web technology. URL, markup languages (Hyper Text Markup Language (HTML), eXtensible Markup Language (XML)), the HTTP protocol is another component which improve scalability, security and performance System.

5.6 Multi-tenant technology

The same application logic is simultaneously accessible more users using multi-tenant technology. Multi-tenant applications ensure that each tenant has its own separate view application and tenant have not allowed data access and applications to other tenants. Each tenant can independently manage their application features, such features are user interface, business process, data model and access control. The most common feature of a multi-tenant application is usage isolation, data recovery, data layer isolation, data security, application upgrades, system scalability and metered usage.

5.4 Service technology

Service technology is the fundamental foundation of the cloud computing that is used to create cloud-based delivery "as a service". models. Web Service, REST Service, Service Agents and service middleware are core technologies for building cloud environment. Web service description language (WSDL), an XML Schema Definition Language, a simple object Access Protocol (SOAP) and Universal Description, Discovery, and Integration (UDDI) are standards originating from the first generation of web services. Like web services, REST the service does not have a separate standard interface. Residue the service shares a common interface that is usually created using the HTTP protocol. A common interface known as unified contract/interface, client-server, stateless, cache, layered system and code on demand are six restrictions in REST services



Security topic	Security issues	Studies/survey	Security solutions
Cloud to cloud trust	Invalid enterprise trust model Cloud environment openness	[12] [54]	Cloud Trust Authority provides security of the cloud services from multiple providers [61] Use different trust models [188]
Human aspect	Un-trusted employees Password sharing Password strength and commonness Social engineering Phishing attack	- [168] [42] [51] [94]	Public Key Infrastructure based trust model Evidence based trust model
Reputation	Isolation of reputation Fate-sharing	[47] [111] [34] [135]	Reputation based trust model SLA verification based trust model Evidence based trust model
Trust on the audit-ability reports	Providers reports truthfulness Jurisdictional audits, court system Data locality Lack of privacy capable audits techniques	[55] [34] [196] [135]	Policy based trust Use cloud auditor's assessment Accreditation by Auditing Standards Board of AICPA
Anonymization	logs anonymization	-	LKC privacy model [109] Data Anonymization [142]

6.CLOUD SECURITY ISSUES

In this part, the work mainly focuses on several categorized security problems and their solutions. First, the work presents a brief introduction about the security issue in cloud computing then they present their solutions. A security issue is something happening in any asset - attacks, misconfiguration, error, damage, loopholes and weakness in the system. There's a lot of it the difference between a specific cloud problem and a general problem. The Cloud related issue is generated due to properties cloud computing, defined by NIST and is much more difficult implement security solutions in a cloud environment. The survey categorized the security issue into eight parts as data issues of storage and computing security, virtualization security problems, Internet and services related security problems, network security issues, access control issues, software security issues, trust management issues, compliance and legal aspects. The overview is summarized in Figure 2. Figure 2 creates a building block in the reader's mind to help understand current security issues. Presented data store and computer, virtualization, and platform-related issues fall under cloud delivery models. Addition, survey on Internet-related issues. Finally a survey cover security issues related to trust and legal issues.

6.1 Data storage and computing security issues

Data is an important part of cloud computing. Data stored in the cloud is isolated and unfathomable to customers. Customers on the one hand, they are either reluctant to provide theirs information or are constantly worried about losing their data bad hands, adverse consequences that can occur during handling and processing. So their data should be consistent during computation, confidential at every stage processes and permanently stores for the purpose of updating records.

The main problem is remote or third-party storage is that the user does not know what happens after saving data in the cloud. The owner of the data does not know cloud storage location, security services and security mechanisms used to secure cloud data. Quality of service is an important aspect in the cloud storage space. A cloud storage provider needs the right technology and mechanisms for efficient and reliable data storage cloud. There are two situations before the calculation

Data storage The problem with data storage is the loss of control a major problem in the cloud computing model because it is not it provides full control over the data and is harder to audit data integrity and confidentiality. Cloud customer computing is physically separated from their data, storage and computing server. Cloud computing is provided by the server pool that stores cloud data. The location of the server pool it is anonymous and is controlled and managed by a cloud service provider. Abstracting the virtual layer makes it difficult find the actual location of the storage server. User allows some level of control only on virtual machines. Characteristics cloud computing, such as multi-tenancy and virtualization give the attacker more options to carry out the attack. User data is stored in cloud data centers. Many a big player provides cloud storage at a very cheap competitive price costs. This distributed data is highly redundant and stored on different physical locations. Redundancy of the electrical source and efficient cooling ensure high data availability.

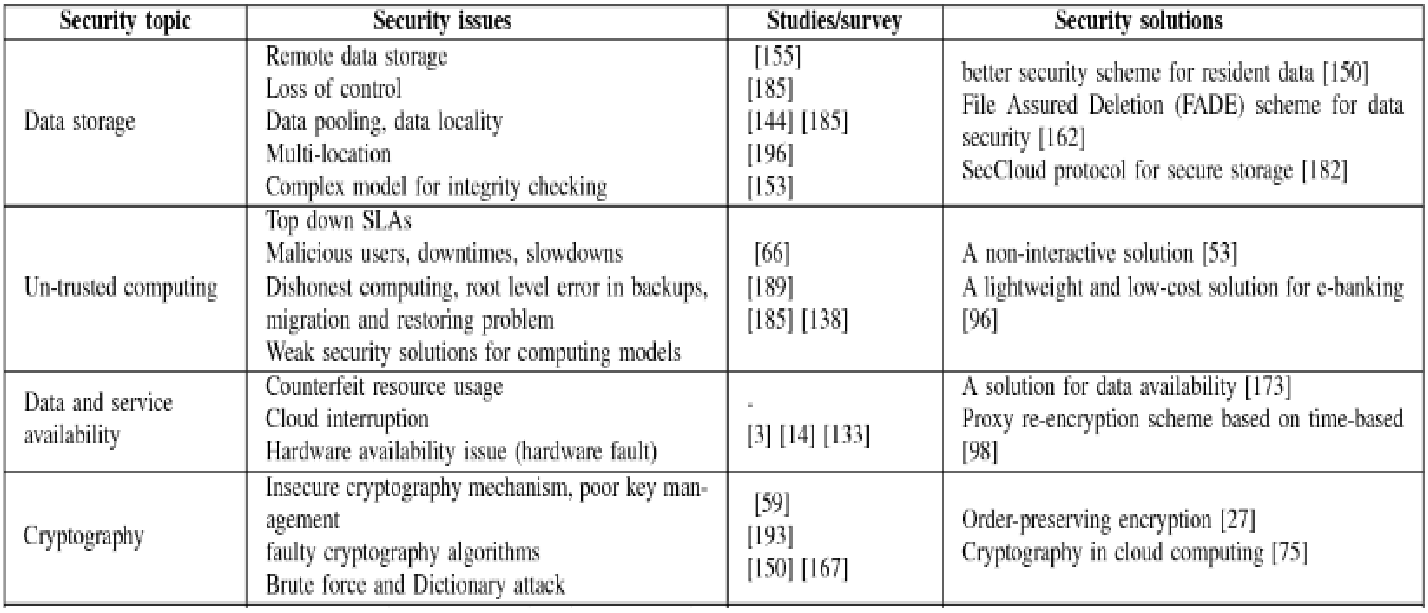
Using the right space allocation mechanism, the cloud the space can be effectively reused. It ensures data redundancy a mechanism in which data is backed up to another cloud server to ensure high data availability. In the case of one the data center has completely failed, the provider is using backed up data server. Google and Amazon have different data servers different countries. These organizations store their data on the basis of the multi-location feature that can bring new security threats and legal issues such as data stored around the world they have different policies.

Cryptography Cryptographic mechanisms are used secure cloud information and data. It is a direct direction an idea to achieve cloud security. Converts simple text data into another form of text called ciphertext. The a notion based on the assumption that it is infeasible to calculate plaintext data value if ciphertext is available.

So they require careful and strong implementation cryptographic methods, because the whole security depends on it to the key that is used as the encryption key. First class factoring a large number gives more security Encryption based on Rivest Shamir Adleman (RSA). They are cannot be computed in discrete logarithmic time. Poorly implementation of the algorithm or uses a weak key v encryption increases the possibility of attack. The most common attack in cryptography is a brute force attack, match anything possible keys with an encryption key in a known range

Cloud data recycling It was a wise suggestion to reuse cloud space once the data is properly utilized and sent to waste. However, it must be ensured that the data used from the previous user is not available to the next user. The the process of cleaning or removing a particular piece of data the resource is known as sanitation. After sanitation updated data is available to people in a distributed manner.

Data sanitization is a critical task in a distributed system for the purpose of proper data disposal and data collection which it is sent to the trash. Improper sanitation provides data may leak and lose data because the hard drive may be deleting some important data.

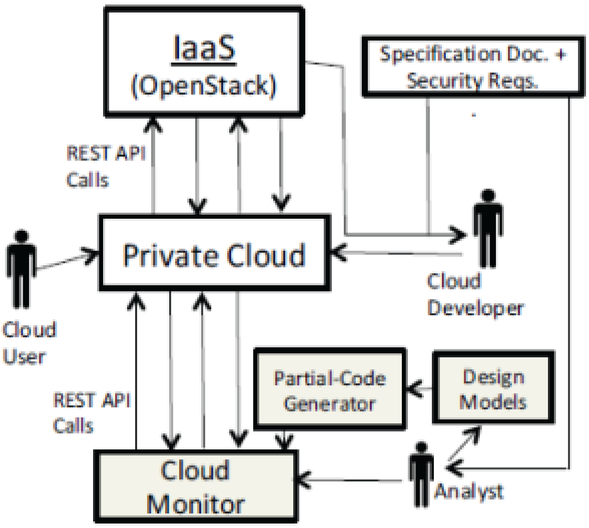


Security topic	Security issues	Studies/survey	Security solutions
Data storage	Remote data storage Loss of control Data pooling, data locality Multi-location Complex model for integrity checking	[155] [185] [144] [185] [196] [153]	better security scheme for resident data [150] File Assured Deletion (FADE) scheme for data security [162] SecCloud protocol for secure storage [182]
Un-trusted computing	Top down SLAs Malicious users, downtimes, slowdowns Dishonest computing, root level error in backups, migration and restoring problem Weak security solutions for computing models	[66] [189] [185] [138]	A non-interactive solution [53] A lightweight and low-cost solution for e-banking [96]
Data and service availability	Counterfeit resource usage Cloud interruption Hardware availability issue (hardware fault)	- [3] [14] [133]	A solution for data availability [173] Proxy re-encryption scheme based on time-based [98]
Cryptography	Insecure cryptography mechanism, poor key management faulty cryptography algorithms Brute force and Dictionary attack	[59] [193] [150] [167]	Order-preserving encryption [27] Cryptography in cloud computing [75]

7.RESEARCH AND DESIGN

In the project, cloud developers are building private clouds using Infrastructure as a Service (Iaas) via REST APIs. For each request and response pattern, evaluate the request using the checkers tool to generate the pattern, and then validate the request. Build part of the code based on the results analysis. After successful authentication, Cloud Monitor provides access to cloud users in a response format (for example, 2xx format) where it identifies the valid request from the REST API.

If it is an invalid request, Cloud Monitor responds in 3xx / 4xx format, restricting access to unauthorized users. If an error is found, it generates a 5xx response type.



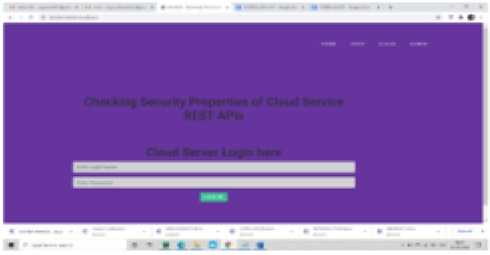
8.ACKNOWLEDGEMENT

We would like to thank Anthony M. Rutkowski, ITU-T Q.4/17 Rapporteur, of Yaana Technologies, Inette Furey of DHS, Damir Rajnovic of FIRST/Cisco Sys tems Ltd., Robert A. Martin of MITER Corporation, Gregg Schudel of Cisco Systems Ltd. and Craig Schultz from Multimedia Architectures for their many helpful comments and their insightful review of our first draft. We also
I want to thank Toshifumi Tokuda of IBM, Hiroshi Takechi
by LAC and SeonMeyong Heo of BroadBand Security, Inc. for their very helpful suggestions.

11.RESULT

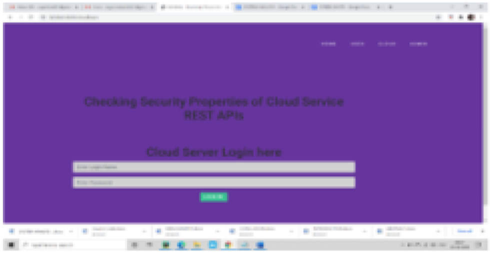
Here we run the code to display a page where the user can register with the required credentials. User content is approved and enabled by the administrator. The administrator contains the user details provided by the user. The user can also create an application to store their notes or information.

The user's opening of the application is confirmed by the cloud.


Checking Security Properties of Cloud Service
REST APIs

Cloud Server Login here

This is the home page of user. Here, User can upload the files in app. And also can view the files. User can only upload files, edit/update and access the files only in user page. User is not allowed to edit or upload files except download files from cloud and admin.


Checking Security Properties of Cloud Service
REST APIs

Cloud Server Login here

This is the cloud server login page. Cloud server activate the user app and generates secret key. Every user has unique secret key. By the key user's data is protected by the cloud server from other users.

9.DISCUSSION

REST API'S is the newest technology and not much is known about it. In addition to the lack of knowledge, there are many uses. While our work in this article represents pure creativity in solving new problems.

10.CONCLUSION

Cloud computing provides the advantage of rapid deployment,
cost efficiency, large storage space and easy access to system anytime, anywhere. So cloud computing is very evident technology appeared quickly and widely recognized computing environment worldwide. However,
there are many security and privacy concerns that prevent this
adoption of cloud computing. All cloud users should be well aware of existing vulnerabilities, threats and attacks in the cloud. Awareness of security threats and attacks will help organizations quickly adopt the rate
cloud. Cloud computing uses many traditional like
and new technologies. These emerging technologies can

create many cloud-specific security issues. Multi-tenancy a The cloud's virtualization feature allows its user access to the same physical resources from different locations. Absence proper isolation between VMs can compromise security system.

In this article, we have discussed the basic features cloud computing and also the security issues that arise due to its virtualized, distributed, shared and public nature cloud. Subsequently, another counter was presented in the post measures to solve security problems in various areas cloud. Tabular presentation of security attacks, threats, problems and their solution will be of great help to the readers. On the last part of the post, a discussion of some open questions in the cloud will motivate researchers and academia to focus on it Subject.

12. REFERENCES

[1] Abbas A, Khan SU. A review on the state-of-the-art privacypreserving approaches in the e-health clouds. Biomedical and Health Informatics, IEEE Journal of. 2014 Jul;18(4): pp. 1431-1441.

[2] Aguiar E, Zhang Y, Blanton M. An overview of issues and recent developments in cloud computing and storage security. InHigh Performance Cloud Auditing and Applications 2014 Jan 1 (pp. 3-33). Springer New York.

[3] Ahuja SP, Komathukattil D. A survey of the state of cloud security. Network and Communication Technologies. 2012 Nov 20;1(2): pp. 66-75.

[4] Aihkisalo T, Paaso T. Latencies of service invocation and processing of the REST and SOAP web service interfaces. InServices (SERVICES), 2012 IEEE Eighth World Congress on 2012 Jun 24 (pp. 100-107). IEEE.

[5] AlFardan, N., Bernstein, D., Paterson, K., Poettering, B., Schuldt, J.: On the Security of RC4 in TLS.http://www.isg.rhul.ac.uk/tls/ index.html(2013). Accessed December 2015.

[6] Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015 Jun 1;305: pp. 357-383.

[7] Almorsy M, Grundy J, Mller I. An analysis of the cloud computing security problem. InProceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010 Nov.

[8] Amazon: Amazon Elastic Compute Cloud (Amazon EC2).https:// aws.amazon.com/ec2/(2012). Accessed November 2015.

[9] Amazon: Amazon Virtual Private Cloud (Amazon VPC).http:// aws.amazon.com/vpc/(2012). Accessed November 2015.

[10] Amazon: Amazon Web Services: Overview of Security Processes. http://s3.amazonaws.com/aws blog/AWS Security Whitepaper 2008 09.pdf(2011). White Paper. Accessed November 2015.

[11] Amazon Web Services Discussion Forums: Low Entropy on EC2 Instances Problem for Anything Related to Security. https://forums.aws.amazon.com/thread.jspa?messageID=249079(2011). Accessed November 2015.

[12] Amoroso EG. From the enterprise perimeter to a mobility-enabled secure cloud. Security & Privacy, IEEE. 2013 Jan;11(1): pp. 23-31.

[13] Anala MR, Shetty J, Shobha G. A framework for secure live migration of virtual machines. InAdvances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on 2013 Aug 22 (pp. 243-248). IEEE.

[14] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM. 2010 Apr 1;53(4): pp. 50- 58.

[15] Armbrust, M., Fox, O., Griffith, R., Joseph, A.D., Katz, Y., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. Above the clouds: a Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28. Electrical Engineering and Computer Sciences University of California 2009.

[16] European Network and Information Security Agency(ENISA). URL http://www.enisa.europa.eu/.

[2] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009.

[17] J. Baker, A. Buttner, and T. Wittbold. Common Result Format (CRF) Specification Version 0.3. URL http://crf.mitre.org/, September 2009.

[18] C. Blanco, J. Lasheras, R. Valencia-Garcia, E. Fernandez-Medina, A. Toval, and M. Piattini. A systematic review and comparison of security ontologies. In The Third International Conference on Availability, Reliability and Security, 2008.

[19] A. Buttner and N. Ziring. Common Platform Enumeration (CPE) - Specification. URL http://cpe.mitre.org/, March 2009.

[20] S. Allamaraju. RESTful Web Services Cookbook. O’Reilly, 2010.

[21] Amazon. AWS. https://aws.amazon.com/.