An experimental study on cloud computing security issues and a framework for xml ddos attack prevention

N.Krishnamoorthy1, Dr.S.Umarani2
1 Research Scholar, SRM Institute of Science and Technology, Chennai (Assistant Professor, Department of Computer Applications) SRM Institute of Science and Technology, Ramapuram Campus, Chennai 89,

2 Research Supervisor, SRM Institute of Science and Technology, Chennai (Professor & Head, Department of Computer Science) SRM Institute of Science and Technology, Ramapuram Campus, Chennai 89

e-mail: 1Krishnamoorthy72srm@gmail.com, 1Krishnan@srmist.edu.in, ravania@gmail.com, hod.dcs.rmp@srmist.edu.in

Abstract. Cloud Computing (CC) is the openness of PC framework assets, especially information stockpiling also, processing power, selective of direct exuberant oversight by the client. In most recent decade, major oddity have gotten known, which gives add more practicality to organizations other than clients. This has seen noteworthy advancement in its working and happen to widely received by either private or public segments. It very well may be seen that more number of associations are communicating their data to the cloud. Alternately, security is a significant caution for the CC administrations which is based on Internet association that makes it vulnerable to different kinds of assaults. In this paper, we do an evaluation concentrate on CC and tended to grouped kind of assaults and likely intimidation to this cutting-edge aptitude, just as stronghold means and clarification to such hit. Cloud Security(CS) is a composite relations of advances, controls, cycles, and approaches.

Keywords: Cloud computing, privacy, challenges, data centres

1. Introduction
The goal of CC is to give consent to users to take advantage from all of these advancements, exclusive of the prerequisite for significant data about or dominance with each and every one of them. The CC plans to trim down the cost and allow the clients to focus on their middle business instead of being hampered by IT boundaries. CC impact on live advances along with the Internet to offer types of assistance to supporters. It has four activity shapes specifically: private, public, network and hybrid

The public cloud is a figuring administration introduced by outsider source over the public Internet, making them open to every individual who wants to utilize or acquire them.
Private clouds are created from software that operate on a part of hardware at the organization. It is set out within the firewall on an organization’s intranet, with an implication that transfer rates are considerably better.

Hybrid cloud is an arrangement with a mix of on-premises, private cloud and outsider, public cloud administrations with the piece connecting the two stages.

A community cloud is a multi-tenant model which permit more than a few companies work on the identical platform, agreed that they have analogous requirements and concerns.
Organizations are needed to impart unswervingly to the cloud and utilize the administrations in pay-by-use offices. This one assists organizations with avoiding capital outpouring on strengthening neighborhood foundation types of gear and immediately raise or psychologist varying [8]. Cloud is an exemplary representation for an available web affiliation which is disguised from clients [9]. The CC is a lot of safe since it is a mix of innovation which gives stockpiling administrations and facilitating on the web.

2. Literature Survey

In 2011, a business related to CC administrations like organizations, stockpiling, workers, administrations and applications without truly accepting them. It is seen that working expense of the cumbersome structure has been zero down of danger, information admit and so on [1].

Jaydip Kumar [2] examined about cloud security that information mounting largely hitherto security of an open finished and fairly effectively accessible chattels is as however flawed and explores perils of danger from circulated figuring condition, characteristics, cloud transport model and the cloud accomplice.

In cloud, multi-divided storage is an important assistance which is utilized for Cloud storage and access information distantly, capacity can encode and store data in various portions of cloud [3] proposed archetypal, that give answer for various insider’s assault, protection to various documents transferred by various clients, and decentralized dissemination of information stockpiling utilizing a file based cryptographic information.

In 2018, CS become annoying for cloud scientists due to unapproved acts are developing on as per CC [4] suggested different security plan for cloud skeleton that present extra safe information transform and defend from surge. Information owner and cloud workers have assorted qualities, this structure present data accumulation and have different security issues, a self-deciding strategy is important to confirm that cloud data is encouraged precisely in the cloud [5] examined diverse security procedures for secure information stockpiling on cloud. CC assurance is a significant and essential reality, has uncommon disputes and issue interconnected it [6] explained the rundown of elements that are exaggerated the security and review safety disputes and concerns are experienced by cloud specialist co-op and purchasers like information protection, Problems with defence and tainted application.

Mrs. Asma A. Shaikh et.al[7] examine about disputes of distributed computing security, XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and its likely countermeasures

The security issues over the Internet incorporate disavowal of administration, listening in, IP–caricaturing based flooding and disguising, while answer for these incorporate secure attachment layer, cryptography, interruption anticipation frameworks and computerized endorsements. This paper analyzes the difficulties and IP–caricaturing based flooding and disguising lastly present a diagram of XML SOAP exhibit assaults.
3. Different Types Of Attacks

3.1 IP Spoofing

IP spoofing is the establishment of Internet Protocol (IP) packets which have a custom-made source address in order to either conceal the uniqueness of the dispatcher, to pretend to be a different computer system, or both. It is a practice habitually used by dreadful player to invoke DDoS attacks against a device.

![Figure 5: IP spoofing](image)

3.2 DDoS Target Attack

It is a vindictive undertaking to upset normal traffic of an ambushed worker, administration or organization by overwhelming the objective or its encompassing foundation with a surge of Internet traffic. It needs a trespasser to oversee an organization of online devices so as to complete an assault.

![Figure 6: DDoS attack](image)

3.3 XML Based Denial Service Attacks

Hash collision attack (Hash DoS): Outsized POST loaded by voluminous structure factors is sent, which require hodgepodge linked preparing
XML external entity DoS: These powers the provider to determine an enormous outer substance characterized in a DTD

XML entity expansion: “XML bombing”, through settling ability of XML

Oversized cryptography: Attacker appends enormous measures of the encoded or carefully marked pieces in message.

WSDL scanning: It is a publicizing technique aimed at network administrations to determine the boundaries used to associate the particular strategies. The data indicated by a WSDL interface uncovers delicate data, which permits the aggressor to dispatch different assaults.

Metadata ridiculing: This assault is expected to re-engineer the web administration's metadata depictions.

Attack obfuscation: Consumes XML encryption to cover content of message from being reviewed by the firewall or IDS. These encoded substance can be utilized to dispatch different assaults, for example, gigantic payload, strong analysing or XML infusion, and encryption

Business Process Execution Language (BPEL) state deviation attack: It gives the web administration final points, which acknowledge the administration demand.

Instantiation flooding attack: When another solicitation message shows up, another occurrence of the BPEL cycle is made and completes the directions given in the procedure depiction.

Aberrant flooding: This assault is conceivable in light of the compositionality highlight of the web administration.

Middleware seizing: This assault relate WS tending to satirizing, yet it guides the aggressor's endpoint URL toward a current objective framework running a genuine assistance at the URL determined.

4. Soap Array Attack

Figure 7: Example Structure before SOAP Array attack

Figure 8: Example Structure After SOAP array attack:

Pseudo Code
Hybrid Cloud Trace Back for Cloud Computing:
This snippet will protect the SOAP element from the DDOS and neighbour attacks
HCTB Procedure at HCTB at interface
{
For each inward message x
If no header then
Create SOAPHeaderElement ("Body") invoke new SOAPHeaderElement ("#Body")
Create SOAPHeaderAttribute ("#Id") invoke new SOAPHeaderAttribute ("#Id")
Else
get WSUsernameToken(x)
WSSusername=new clientID()
WSSusername=new ClientName()
WSSsignature=new ClientSignature()
}

Article I. Attack description
SOAP messages are flexible in a few conduct, and Arrays are upheld. Then again these viewpoints that can be broken by a mugger to produce a DoS assault to limit the WS availability. Before utilizing a SOAP exhibit we must be characterize its ability or sizes. Nonetheless, SOAP doesn't restrict the quantity of components inside an exhibit. This property can be mishandled by an intruder to execute a DOS assault restricting the accessibility of the web administration. We should expect an aggressor pronounces a cluster with 10,000,000,000 String components. Preceding the message is handled, the WS will assign space for 1,000,000,000 String Elements in the RAM. Generally that will make a memory breakdown of the assaulted framework. Simple anticipation methodologies exist in the event that one is ready about the issue.

Article II. Fundamentals for attack
We must have an idea of the facts
1. Attacker knows endpoint of web service: WSDL isn't required, on the grounds that the attack is only settled on the XML Parser.
2. Attacker can reach endpoint from its location: Right of passage to the focused on WS is basic. In the event that the WS is just offered to clients inside a clear gathering, the attack is least.

Article III. Attack example
Here, we consider an random SOAP message with a string array. In this case the invaders announce a SOAP array with ten crore elements.

Article IV. Attack modification and countermeasures
The assault can be hindered by utilizing harsh blueprint approval. As a rule cases the constraint of cluster components is known. In this model We envision that only 10 components are endorsed, not more than that. For this situation an appropriate construction is

```xml
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Body>
    <ws:FunctionWithArrayInput unencoded="...">
      <DataSet arrayType="xsd:string[1000]">
        <item xsi:type="xsd:string">value1</item>
        <item xsi:type="xsd:string">value2</item>
        <item xsi:type="xsd:string">value3</item>
      </DataSet>
    </ws:FunctionWithArrayInput>
  </soap:Body>
</soap:Envelope>
```

Coding part 1: SOAP Message with unencoded Array in body

```xml
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Body>
    <ws:FunctionWithArrayInputBAT unencoded="...">
      <DataSet arrayType="xsd:string[1000]">
        <item xsi:type="xsd:string">value1</item>
        <item xsi:type="xsd:string">value2</item>
        <item xsi:type="xsd:string">value3</item>
      </DataSet>
    </ws:FunctionWithArrayInputBAT>
  </soap:Body>
</soap:Envelope>
```

Coding part 2: Selection of permanent XML Schema

```xml
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Body>
    <ws:FunctionWithArrayInputB unencoded="...">
      <DataSet arrayType="xsd:string[1000]">
        <item xsi:type="xsd:string">value1</item>
        <item xsi:type="xsd:string">value2</item>
        <item xsi:type="xsd:string">value3</item>
      </DataSet>
    </ws:FunctionWithArrayInputB>
  </soap:Body>
</soap:Envelope>
```

Coding part 3: Constraining a valid SOAP message
On the off chance that we can’t limit the amount of components per default, one more answer can be started. So it is standout to assess the amount of expressed components in the "soapenv_arrayType" trait with amount of solid dynamic exhibit components. On the off chance that they are not identical, the SOAP message is undesirable.

5. Conclusion
Currently limitless economic setbacks to the sufferer party are created by one of the largely universal cyber-attack mode namely the DoS. A particular elucidation that is suitable for the entire means regrettably is unsuccessful to forestall DDoS assaults, which are still increasingly hitting the harmless cloud user. However the latest technologies also involve an important part in avoidance of such intimidation. This can be completed by elevating shield measures that incorporate anticipation, recognition, improvement and reaction methods. As CC grows in leaps and bounds every day, equivalently DDoS attacks becomes more complicated to the possibility that can beat a cloud provider.

As there are DDoS attacks on escalation in all budding technologies, we can expect in the impending, that countless weakness and the corresponding security methods will also raise.

The subsequent methods have to be taken against DDoS attacks
1. Observing interior (internal) network message flow and practice of server properties, such as DNS and web server, to discover premature traffic increases and anomalous consumption of system assets.
2. Assessing Login checking alarms produced by Intrusion Detection System (IDS) Internet gateway and firewall, to detect doubtful actions.
3. We can deploy our network in such a way that bifurcates critical activities are handled separately in a network besides an usual connection for other essential activities.
4. We can adapt a policy strengthening security practices to deny needless network transfer. For example, preventing unwanted and malicious entries, and request from illegal network devices.
5. Performing frequent audit trials and security checks in the organization network
6. By adapting strong XML Digital Signature methodologies

Abbreviations used:

| CC     | CLOUD COMPUTING |
|--------|----------------|
| DDoS   | Distributed Denial-of-Service |
| DoS    | Denial-of-Service   |
| DTD    | Document Type Definition |
| WSDL   | Web Services Description Language |

References
[1] R. Choubey, R. Dubey, and J. Bhattacharjee, “A survey on cloud computing security, challenges and threats,” Int. J. Comput. Sci. Eng., vol. 3, no. 3, pp. 1227–1231, 2011.
[2] Jaydip Kumar-Cloud Computing Security Issues and Its Challenges: A Comprehensive Research-International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-154, June 2019
[3] K. Subramanian and F. L. John, “Secure and Reliable Unstructured Data Sharing in Multi-Cloud Storage using the Hybrid Crypto System,” IJCSNS, vol. 17, no. 6, pp. 196–206, 2017.
[4] A. Hussain, C. Xu, and M. Ali, “Security of Cloud Storage System using Various Cryptographic Techniques,” International Journal of Mathematics Trends and Technology ( IJMTT ), vol. 60, no. 1, pp. 45–51, 2018.
[5] A. Venkatesh and M. S. Eastaff, “A Study of Data Storage Security Issues in Cloud Computing,” IJSRCSEIT, vol. 3, no. 1, pp. 1741–1745, 2018.
[6] G. Jain and A. Jaiswal, “Security Issues and their Solution in Cloud Computing”, Concepts journal of applied research(CJAR), vol. 02, no. 03, pp. 1-6, 2018
[7] Mrs. Asma A. Shaikh--Attacks on Cloud Computing and its Countermeasures
International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016-978-1-5090-4620-1/16/$31.00 ©2016 IEEE

[8] Joonsang Baek, Quang Hieu Vu, Joseph K. Liu and Yang Xiang “A secure cloud computing based framework for big data information management of smart grid,” IEEE transactions on cloud computing 3.2, 233-244, 2015.

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