

Security issues in cloud, fog and edge computing models and suggested solutions

Krishan Kumar *

Dinesh Kumar Saini †

Department of IoT and Intelligent Systems

Manipal University Jaipur

Jaipur

Rajasthan

India

Abstract

This investigation on data and information security in cloud, fog and edge computing explores the essential security challenges and solutions in all three computing paradigms. We identify the gaps between current security requirements and the state-of-the-art security solutions. Security gaps eventually lay path to areas for future research in cloud security. During this investigation, we study and analyze existing cloud, Fog and Edge security solutions and figure out their limitations to address current security issues.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Cloud computing, Cloud security, Vulnerabilities, Threats, risks, Hybrid cloud, Public cloud, Private cloud, Virtualization, Hypervisor.

1. Introduction

Cloud computing is a very popular and cost-effective model of computing that has emerged as a boon for small and medium enterprises. But nothing comes without downsides so does cloud computing. Data security and customer's control over data are main challenges cloud computing surfaces. Same challenges are faced by cloud computing extensions like FOG and Edge. Data security and data control are the main apprehensions of customers when they move to cloud services. And there

* E-mail: aapkakk@gmail.com (Corresponding Author)

† E-mail: dksssohar@gmail.com

is no great trust model except cloud-service-provider’s reputation and perception, which cloud-customers can use to evaluate service-provider’s quality of services [1]. As part of this paper, we propose trust metrics for cloud security those eventually be used to create a universal trust model for cloud services.

2. Cloud Computing

The word “cloud” is symbolically used for internet and cloud computing refers to the delivery of computing services over the internet, providing users with access to a variety of resources such as servers, storage, databases, networking, software, and more, without the need for on-site infrastructure or maintenance [2]. Instead of owning and managing physical hardware, users can leverage cloud services from providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others.

There are four types of cloud deployment models that provide cloud services to different categories of cloud customers. Those models are- Public, Private, Hybrid, and Multi Cloud.

And, there are three services provided by cloud computing - Software, Platform, and Infrastructure as a Service. This service model is collectively called SPI model. Apart from these three services, few companies provide some specific services in cloud like, Oracle provides Database as a Service (DBaaS). DBaaS allows customers to quickly create a service instance in the Oracle Database Cloud.

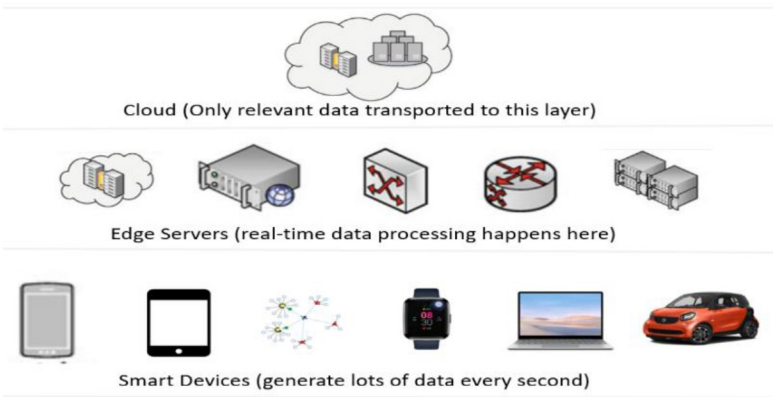


Figure 1
Taxonomy of edge computing framework

3. Edge Computing

Edge computing refers to the practice of processing data closer to the source of data generation. These data generation sources are individual smart mobile or IoT devices that consistently generate big volume of data.

Edge computing is new computing model where computing service is brought closer to data generation source. Edge devices are smart, they can process the data they collect and make appropriate decisions. Figure 1 shows the taxonomy of edge computing framework.

According to Gartner, by the year 2025 almost 75% of data generated by IoT will be processed outside centralized cloud datacenter [3].

4. Fog Computing

Fog computing is a decentralized computing infrastructure in which data, compute, storage, and applications are distributed in the most logical, efficient place between the data source and the cloud. Like edge computing it is another architecture that is extension of cloud-computing service to the edge network. Fog computing aims to address the limitations of traditional cloud computing architectures by leveraging distributed resources at the edge of the network to meet the demands of modern applications and services. [4].

Fog computing helps saving network bandwidth and operates on low latency because it does not send all data to cloud. It reduces data traffic by doing intermediate processing at certain access points.

5. Background of Cloud Security

The problem of data security in computers is not new. In early times, threats were physical in nature like unreliable media (floppy disks and cd drives) and natural disasters, but they were old problems. With the rapid evolution of networking and internet, data and information security scenario has changed. Now, all security solutions must address data and information security in networked environment [5].

Rapid growth of cloud computing in last decade has posed new security challenges before computing world.

6. Problem Area in Cloud Security

Cloud computing is a centralized computing model along with storage and network infrastructure. In cloud computing all customer data

On Premise	IaaS	PaaS	SaaS
Physical Assets	Physical Assets	Physical Assets	Physical Assets
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Networking	Networking	Networking	Networking
Operating System	Operating System	Operating System	Operating System
Applications Software	Applications Software	Applications Software	Applications Software
Data	Data	Data	Data
Access Control	Access Control	Access Control	Access Control
Cloud Customer Responsibility		Cloud Service Provider Responsibility	

Figure 2

CC and CSP's responsibilities for cloud security

are transported to cloud for processing and storage. Customers have no control over the data storage location; therefore, they must completely trust on what is promised by CSP. Figure 2 shows the shared responsibility for cloud security.

Edge computing offloads computing close to the data generation source. This distributed computing model reduces physical distance between enterprise applications and data sources [6]. Reduced distance between data source and computing infrastructure delivers two major benefits - better response time and bandwidth availability.

Like edge computing, fog computing is another data computing model that came from Cisco aiming to promote IoT scalability, where huge data is generated by IOT devices that needs to be processed in real-time.

7. Data Security in Cloud Computing

Data security in cloud is a great concern because CCs have no or little control over their data (especially in public clouds). Therefore, it is essential to ensure the security of customer's data. In cloud computing, data security is a phenomenon of utmost priority. Ensuring security does not only reduce the cloud attack surface but also improve CC's confidence for opting cloud services [7].

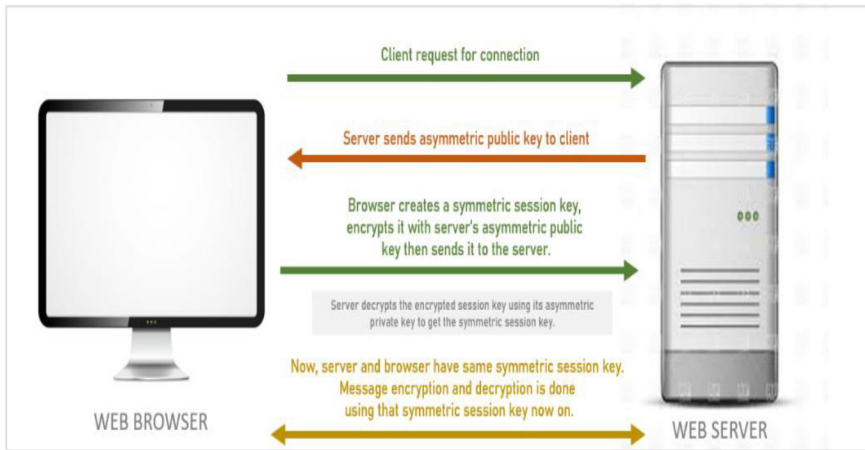


Figure 3

Use of asymmetric and symmetric encryption in SSL

Confidentiality, integrity, and availability are three main components of all data security models. Every security solution must implement these components.

Confidentiality hides sensitive data from unauthorized users.

Integrity ensures that unauthorized user should not be able to alter or temper system state and data.

Availability ensures that data is consistently available to authorized users even when there is any component failure.

Confidentiality and privacy are the biggest concern of SaaS customers. All customers undoubtedly want their business and personal information confidential on cloud [8]. Cryptography is the most widely used mechanism to maintain confidentiality of data in cloud. Encryption, Digital Signatures, and TLS/SSL are the basic techniques of data security over the network.

Figure 3 shows how SSL uses both asymmetric and symmetric encryption in HTTPS protocol.

7.1 Data Security in Fog

Fog computing offloads computing and storage closer to data generation source or router. This helps reducing latency and provide computing service more swiftly [9]. Fog computing has following security issues.

- **Account hijacking** means malicious users intentionally attack user accounts to gain access using phishing techniques.

- **Denial of service (DoS)** happens when hackers get access to the system and make the entire system either inaccessible or very slow.
- **Data breaches** is very common attack in cloud, where hackers get unauthorized access and temper customer's sensitive data stored in the cloud.
- **Data loss** is caused when hackers get access to system and corrupt or delete customer's data.
- **Malicious insiders** are authorized users with bad intentions who cause harm, damage, or steal customer's data.
- **Insufficient due diligence (IDD)** means there is no concrete plan and accurate policies to reach security goals. IDD is a big security glitch in cloud computing environment.

7.2 Data Security in Edge

There are two major challenges in edge computing – implementation of edge computing and security & data privacy.

As we know, in a network every device is given a name and ip address to recognize that device in network. In edge computing, we need a strong naming scheme to handle dynamic network topology and the mobility of nodes, and security issues. Old schemes like DNS cannot handle the dynamic nature of edge network.

Other privacy issues like poor credentials for edge devices, insecure communication, backup and recovery and poor network visibility are also big cause of concern in edge computing [10].

8. Trust Models for Cloud, Edge, and Fog Computing

Trust is established between cloud service customer and CSP based on what is promised and what is delivered by CSP. Quality of service and CSP's reputation also play very important roles in winning customer's confidence.

8.1 Trust Models for Cloud

While purchasing and using cloud services, customer satisfaction highly depends upon QoS attributes like availability, reliability, and customer support [11]. Table 1 lists down most notable trust models for cloud services.

Table 1
Various trust models for cloud services

Model Basis	Model Type	
Feedback Based Trust Model [12]	Direct Trust Model	
	Indirect Trust Model	
Trust Models Based on Framework	Qualitative Trust Model	
	Quantitative Trust Model	Agent Based Trust Model
		Log Based Trust Model
		Authentication Based Trust Model
Attribute Based Trust Model		

8.2 Trust Models for Edge

Security risks in edge nodes are much higher compared to cloud infrastructure because edge nodes are heterogeneous in nature. Message tampering, replay attacks, and forging are common issues in edge networks, which discourage users from utilizing edge nodes for computing.

8.3 Trust Models for Fog

Trust models in fog computing are important in context of privacy, security, user experience and usability. There are trust models based on subjective logic, trust-based privacy preserved approach. The trust-based privacy-preserving trust model is based on experimental results and trace-driven security analysis that preserves privacy of the nodes while analyzing trust scores.

9. Trust Model for Cloud - Proposed Trust Metrics

To calculate a measurable trust-score we need security metrics, and those security metrics should be universally measurable. If we cannot measure something, we cannot improve and optimize it. Therefore, security metrics should have following attributes.

- Quantitative
- Objectivity
- formal modeling
- time dimension attribute

- Globally acceptable
- Inexpensive
- Obtainable
- Should be Repeatable.

10. Trust Models for Cloud, Edge, and Fog Computing

We propose a hybrid model that is a combination of Weighted Average and Metric Merit Model. We are taking Metric Merit model into account because if high merit metric is compromised then fail the system altogether. For example, encryption metric is a high merit metric, if any service provider does not encrypt that data in use, motion and rest then trust score will be very low. Table 2 contains all the metrics that we are going to use for the trust score calculation model.

Table 2
Trust score metrics table

Metric Name	Metric Weight	Metric Merit	Failure Factor (ff)	Total Weight (Metric Weight * Metric Merit) * ff
TLS/SSL	10	25	0/1	250 * ff
Encryption	10	24	0/1	240 * ff
Access Control	10	23	0/1	230 * ff
Input Sanitization	10	22	0/1	220 * ff
Digital Signatures	10	21	0/1	210 * ff
Hashing	10	20	0/1	200 * ff
No. of weak passwords (non-compliant)	10	19	(T-F)/T	190 * ff
Successful/unsuccessful logons	10	18	(T-F)/T	180 * ff
Unauthorized user access presentation	10	17	(T-F)/T	170 * ff
Information modification presentation	10	16	(T-F)/T	160 * ff
Multi-head approval for information modification	10	15	(T-F)/T	150 * ff

Contd...

Consistency metric score	10	14	$(T-F)/T$	$140 * ff$
No. of Policy Violations	10	13	$(T-F)/T$	$130 * ff$
No. of wrong roles assignment	10	12	$(T-F)/T$	$120 * ff$
No. of delayed software updates	10	11	$(T-F)/T$	$110 * ff$
No. of delayed backups	10	10	$(T-F)/T$	$100 * ff$
Network failover	10	9	$(T-F)/T$	$90 * ff$
High Availability	10	8	$(T-F)/T$	$80 * ff$
No. of incidents blocked	10	7	$(T-F)/T$	$70 * ff$
No. of viruses blocked	10	6	$(T-F)/T$	$60 * ff$
No. of patches applied	10	5	$(T-F)/T$	$50 * ff$
No. of spam blocked	10	4	$(T-F)/T$	$40 * ff$
No. of virus infections	10	3	$(T-F)/T$	$30 * ff$
No. of port probes	10	2	$(T-F)/T$	$20 * ff$
Traffic analysis score	10	1		$10 * ff$
Total Score				CS
Trust Score in %	$(CS / ((N * (N + 1)) / 2)) * 100$			
Legends	T = Total attempts F = No. of times failures occurred N = Number of metrics (25 in this case) CS = Sum of last column <i>Total Weight</i> (<i>metric weight * metric merit</i>) * ff			

Table 3 describes how secure a cloud is and what types of data that can be stored in cloud depending upon the trust score.

Table 3
trust score grades based on hybrid trust model

S. No.	Trust score calculated from table 2	Trust Grade	Good for types of data stored
1.	91% and more	A	Confidential, internal, restricted, and public
2.	81% - 90%	B	Public, internal, and confidential but not restricted
3.	71% - 80%	C	Public and internal
4.	Lower than 70%	D	Public

11. Open Research Issues

In the future, along with the number of smart devices the amount of data will also increase enormously. Further research in this area will revolve around three main areas - (1) reduce latency as much as possible without compromising with reliability, (2) Security and privacy of user data at all layers of the network and (3) support for heterogeneous devices in edge and fog networks.

References

- [1] X. Ma and X. Li, "Trust evaluation model in edge computing based on integrated trust," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. (2018). doi: 10.1145/3302425.3302491.
- [2] "NIST Cloud Computing Program - NCCP | NIST." Accessed: Mar. 03, 2022. [Online]. Available: <https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp>
- [3] Rob van der Meulen, "What Edge Computing Means For Infrastructure And Operations Leaders." Accessed: Mar. 26, (2022). [Online]. Available: <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders>
- [4] Z. Mahmood, *Fog computing: Concepts, frameworks and technologies*. Springer International Publishing, (2018). doi: 10.1007/978-3-319-94890-4.
- [5] M. P. Morolong, F. B. Shava, and A. M. Gamundani, "Cloud computing security in health cyber physical systems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1553–1568 (2023), doi: 10.47974/JDMSC-1821.
- [6] Ryax Team, "Cloud computing vs edge computing - Ryax Technologies." Accessed: Mar. 12 (2022). [Online]. Available: <https://ryax.tech/cloud-computing-vs-edge-computing/>
- [7] Poonia, Ramesh C., and Linesh Raja. "On-demand routing protocols for vehicular cloud computing." In *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing*, pp. 96-122. IGI Global (2021).
- [8] V. Agrawal, N. Dubey, V. Singh, N. Singla, S. Kumar, and D. Goyal, "Authenticated key exchange protocol security of cloud services

- management using machine learning," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1381–1391 (2023), doi: 10.47974/JDMSC-1761.
- [9] S. K. Henge, A. Upadhyay, A. K. Saini, N. Mishra, D. Sharma, and G. Sharma, "Analysis and detection of insider attacks using behaviour rule based architecture in enterprise multitenancy," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 26, no. 3, pp. 707–718 (2023), doi: 10.47974/JDMSC-1743.
- [10] R. Welekar, F. Shaikh, A. Chitre, K. Wanjale, S. Pathan, and A. Kumar, "An advanced cloud based framework for privacy and security in medical data using cryptographic method," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1585–1596 (2023), doi: 10.47974/JDMSC-1826.
- [11] P. Govindaraj, N. Jaisankar, and A. professor, "A reputation based trustworthy system for cloud environment," (2016). [Online]. Available: <https://www.researchgate.net/publication/309671770>
- [12] S. Machhi and G. B. Jethava, "Feedback based trust management for cloud environment," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Mar. (2016). doi: 0.1145/2905055.290533.