

# Chapter 8

## Big Data Issues: Gathering, Governance, GDPR, Security, and Privacy


**Karthika K.**

*Adhiyamaan College of Engineering, Hosur, India*

**Devi Priya R.**

*Kongu Engineering College, Erode, India*

**Sathishkumar S.**

 <https://orcid.org/0000-0003-3825-4148>

*Adhiyamaan College of Engineering, Hosur, India*

### ABSTRACT

*Various unimaginable opportunities and applications can be attained by the development of internet-connected automation. The network system with numerous wired or wireless smart sensors is called as IoT. It is showing various enhancement for past few years. Without proper security protection, various attacks and threats like cyberattacks threat causes serious disaster to IoT from the day it was introduced. Hence, IoT security system is improvised by various security and the management techniques. There are six sections in security management of IoT works. IoT security requirement is described intensively. The proposed layered of security management architecture is being defined and explained. Thus, this proposed architecture shows the security management system for IoT network tight security management for a network of the IoT which is elaborately explained with examples and about GDPR. In information security, intrusion recognizable proof is the showing of placing exercises that attempt to deal the protection, respectability, or availability of a benefit.*

### I. INTRODUCTION

In this advanced period, web has transformed into an essential wellspring of correspondence in pretty much every calling. With the extended utilization of framework designing, its security has created to be

DOI: 10.4018/978-1-7998-3111-2.ch008

astoundingly segregating issue as the workstations in particular affiliation hold private information and delicate data. The framework used to screen the framework security is known as Network recognition. Interruption discovery is to get ambushes against a machine structure. It is a discriminating enhancement great to go part and additionally an element extent of examination.

According to a study by **Faizal M.A. et al. (2010)** a Static Threshold Based Method for Intrusion Detection System is proposed that works for detecting DDOS attacks. The threshold is formulated by set of features that are Timestamp, Duration, IP address of the host being monitored, connection pool, Source and Destination Services, Number of Connections and Status flag of connection. The results are validated by using Statistical Process Control Chart (Shewhart Chart). This intrusion detection system acts on network layer that considers the number of connections made by the attacker which is the main cause of Denial of Services. The TCPDump utility is used to capture the TCP traffic for analysis purposes.

**Gupta et al. (2013)** proposed Profile Based Intrusion Detection System in cloud. This work is based on signature cum behavior based algorithms. The algorithms run for each virtual machine profile and rank the dataset (TCPDump). The dataset is updated and synchronized for new attack patterns regularly for each profile. The use of IP filtering is also incorporated for insider, outsider and malicious intent users. The intrusion detection system implementation is cloud based and uses multiple thresholds to build signature description of each virtual machine. The thresholds are computed on the basis of frequency threshold historically. **François et.al.(2012)** the major work done by these researchers is on TCP Syn flooding attack and most of the features are network based indicators such as bandwidth utilization, packet loss rate, connection type and also include signatures of attacks. **Cepheli et al. (2016)** proposed the intrusion detection system to prevent DDos attacks. **Hwang et al. (2007)** introduced the hybrid intrusion detection with weighted signature. **Xiao et al. (2015)** proposed the approach to detect DDos attack against data center with correlation analysis but detailed mathematical background to compute threshold is neither mentioned, nor there any section in the paper giving details on the method used to validate the results. **Singh et al. (2015)** proposed a data streaming approach to defend against DDos Flooding attacks. **Faizal M.A. et al. (2009)** proposed a threshold based technique for network intrusion detection system. The detection of the intrusion from the normal situation suggested in this work is based on the static threshold. It is obtained from the outcome of observations and experiments. The upper limit and lower limit is calculated by using the sample statistics in which upper control line and lower control line equations are used along with the mean value.

**Hai Ji et al. (2013)** put forward virtual machine monitoring (VMM) based intrusion detection and prevention system named as VMFence. Its role is to monitor the network flow as well as of file integrity. The work states that a privileged VM is used as a centralized architecture to apply the security in the cloud environment. **Jun-Ho Lee et al. (2011)** elaborated a multilevel based DDOS attack detection system which considered the application level traffic only. The authors used anomaly detection management module named as AAA that refers to three keywords authentication, authorization and accounting.

**Jisa David and Ciza Thomas (2015)** introduced a DDOS approach to prevention of attacks on the basis of Current Mean Entropy which is applied on the flow of the network traffic. The approach used the adaptive threshold approach to track the network's activities and behavior of the users. **Praveen Kumar Rajendran, M. Rajesh and R. Abhilash (2015)** discussed the proposed hybrid intrusion detection system for private cloud which is based on empirical research. The authors tested the intrusion detection system on data which is collected by using the network speed. Jmeter is used to calculate the network speed.

**Miao Du et al., (2020)** proposed a training model to protect the big data in smart environment using various algorithms such as OPP and OJP. This paper assurance the perfection on datasets.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/big-data-issues/269560](http://www.igi-global.com/chapter/big-data-issues/269560)

## Related Content

---

### Advanced Data Storage Security System for Public Cloud

Jitendra Kumar, Mohammed Ammar, Shah Abhay Kantilal and Vaishali R. Thakare (2020). *International Journal of Fog Computing* (pp. 21-30).

[www.irma-international.org/article/advanced-data-storage-security-system-for-public-cloud/266474](http://www.irma-international.org/article/advanced-data-storage-security-system-for-public-cloud/266474)

### Advanced Brain Tumor Detection System

Monica S. Kumar, Swathi K. Bhat and Vaishali R. Thakare (2020). *International Journal of Fog Computing* (pp. 31-45).

[www.irma-international.org/article/advanced-brain-tumor-detection-system/266475](http://www.irma-international.org/article/advanced-brain-tumor-detection-system/266475)

### Cloud Analytics: Introduction, Tools, Applications, Challenges, and Future Trends

Hari Kishan Kondaveeti, Biswajit Biswal, Licia Saikia, Udithaa Terala, Sateesh Gorikapudi and Valli Kumari Vatsavayi (2024). *Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models* (pp. 253-267).

[www.irma-international.org/chapter/cloud-analytics/337842](http://www.irma-international.org/chapter/cloud-analytics/337842)

### Key Legal Issues with Cloud Computing: A UK Law Perspective

Sam De Silva (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 2063-2077).

[www.irma-international.org/chapter/key-legal-issues-with-cloud-computing/119947](http://www.irma-international.org/chapter/key-legal-issues-with-cloud-computing/119947)

### Fog Computing Architecture, Applications and Security Issues

Rahul Neware and Urmila Shrawankar (2020). *International Journal of Fog Computing* (pp. 75-105).

[www.irma-international.org/article/fog-computing-architecture-applications-and-security-issues/245711](http://www.irma-international.org/article/fog-computing-architecture-applications-and-security-issues/245711)