Cloud of Things Security Challenges and Solutions

Andras Toth
Signal Department
University of Public Service
Budapest, Hungary
ORCID: 0000-0001-6098-3262

2021 Communication and Information Technologies (KIT) | 978-1-6654-2880-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/KIT52904.2021.9583760

***Abstract*—There are many benefits of combining IoT devices with cloud computing, which can help exploit each service's potential better and increase computing and storage capacity. However, there are also several threats in this area that pose serious security challenges. In this paper, the author has searched for the vulnerabilities and threats specific to the Cloud of Things through keyword analysis, and then completed a deeper analysis of the relevant literature, has identified the security solutions that can contribute to maintaining adequate security of data and services. The focus was on the scientific publications in Elsevier's Scopus database, in which the author sought answers to the following questions: "What are the most common vulnerabilities that threaten the interconnection of IoT solutions and cloud computing?" and "What are the most effective security solutions that can be applied to protect data, devices, and systems in a Cloud of Things solution?". The research results have shown that there are strong links between the threats, which can only be mitigated by a complex and comprehensive security architecture.**

Keywords*—*Cloud of Things, cloud computing, security challenges, IoT vulnerabilities, security solutions

I. Introduction

The Internet of Things (IoT) is a term that is the common name for a high-tech technology that includes sensors, cameras, home, and industrial components (robotic vacuum cleaners, refrigerators, industrial robots, public utilities' metering equipment), smart boards and actuators connected to the Internet. The widespread proliferation of IoT devices is a constant challenge for professionals, demanding ever higher performance, larger storage capacities, and increasing reliability and scalability are essential requirements. As a result, professionals prioritise the interconnection of cloud computing and the IoT ecosystem, including expanding services and the continuous improvement of security levels. With cloud computing, significantly larger storage spaces are available, and different services and applications can be hosted in the cloud and structured as required. All in all, cloud computing provides for users convenient, flexible, and continuously expandable solutions, which makes data and services available anywhere, anytime, with the hardware and software elements available. The main idea is that applications, services, data are not stored, managed, and processed on local servers or computers but on remote devices that can be accessed via the Internet. It can also implement adequate security for different IoT systems.

The research presented in this article is the second part of a larger research project, which is supported by the Hungarian Academy of Sciences and the Ministry of Innovation and Technology. The author examined the general security challenges and threats of IoT devices and systems in the first part. At the same time, the potential applications of IoT in a military environment were analysed, and potential security issues were identified. In this part of the research, the author analysed the relationship between IoT solutions and cloud services.

The universal name for integrating IoT devices and cloud technology is IoT Cloud Computing or Cloud of Things. It is a hybrid solution that provides better access to different resources through the cloud environment. In such smart grids, the individual elements communicate on an equal footing so data can be continuously uploaded and accessed in the systems used. The Cloud of Things is emerging in our daily lives, with smart cities, self-driving cars, and even healthcare deploying elements that use it. Therefore, ensuring adequate security is a major challenge in its deployment. Frameworks have been developed to facilitate Cloud of Things solutions, using different layers such as IoT, Edge, Fog and Cloud Computing. [1]

In this paper, the author has analysed the most common vulnerabilities, threats, and possible security solutions in the Cloud of Things. To get the most accurate and relevant results, the author sought answers to the following research questions during his research:

- What are the most common vulnerabilities that threaten the interconnection of IoT solutions and cloud computing?
- What are the most effective security solutions that can be applied to protect data, devices, and systems in a Cloud of Things solution?

II. Methodology

The author used a literature review and keyword analysis to answer the research questions, focusing on the relevant scientific literature and professional reports. Based on this, the author focused on the following objectives:

- to identify the most common keywords relating to Cloud of Things;
- quantitative analysis based on keyword matches for different threats, vulnerabilities and security solutions;
- comparative analysis illustrating the connexions of each keyword concerning the relevant literature.

Keyword analysis was used to extract relevant information from the analysed literature. The article is divided into the following sections according to the method chosen and the procedure applied:

- defining the relevant literature
- performing keyword analysis
- examination of the obtained results, drawing conclusions.

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-20-5-NKE-5 New National Excellence Program of the Ministry of Innovation and Technology.

978-1-6654-2880-4/21/$31.00 ©2021 IEEE

III. Data

The data for this research were collected from the Elsevier Scopus database. The following research queries were used in the search engine to obtain relevant information on the topic:

- IoT AND "cloud computing" OR "cloud of things" – 6,669 document results;
- IoT AND "cloud computing" OR "cloud of things" AND LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) – 2,126 document results;
- IoT AND "cloud computing" OR "cloud of things" AND LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) AND LIMIT-TO (LANGUAGE, "English") AND LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "ch") – 1,931 document results.

During the keyword analysis, searches were continuously narrowed down to achieve the most relevant results. Accordingly, the author has analysed the literature published in relevant articles, conference proceedings or book chapters over the last two years.

IV. Tools and Analysis

To analyse the links and relationships found in the bibliographic data extracted from the Elsevier Scopus database, the author used the VOSviewer software, which allowed to visualise the structure of the bibliographic and keyword networks, thus facilitating the work to obtain the most relevant information. The research used co-occurrence analysis, which determines the correlation between terms based on the number of phrases co-occurring in the documents. To obtain the broadest keyword network, the analysis of all keyword co-occurrences (all keywords, author keywords, index keywords) was selected.

V. Research

At the beginning of the research, the author examined the most common keywords found in the most relevant papers written on IoT, Cloud Computing and Cloud of Things. The search query returned 1931 documents, of which 996 were found in journals, 571 in conference proceedings, 347 in book series, 17 in books. From these, the author identified the most specific keywords and analysed their most common relationships with each other. As a result, 11277 keywords were identified in the various documents, of which the 25 most frequently occurring are listed in Table I.

TABLE I. The most common keywords in Cloud of Things

	Keyword	**Number of occurrences**
1.	internet of things	1384
2.	cloud computing	1050
3.	fog computing	426
4.	edge computing	346
5.	fog	284
6.	digital storage	225
7.	artificial intelligence	160
8.	network security	149
9.	big data	133
10.	computer architecture	131
11.	energy utilization	121
12.	blockchain	115
13.	information management	114
14.	security	114
15.	quality of service	112
16.	cryptography	111
17.	network architecture	108
18.	data handling	105
19.	machine learning	104
20.	green computing	93
21.	smart city	92
22.	deep learning	91
23.	iot applications	89
24.	5g mobile communication systems	83
25.	energy efficiency	83

As shown in the table above, Fog Computing and Edge Computing are high on the list of keywords. The main reason for this is that these two services can provide important key solutions for Cloud Computing and IoT systems in areas of operations and security. As can be seen in Figure 1, the layers of the Cloud of Things include the cloud, the fog, and the edge computing.

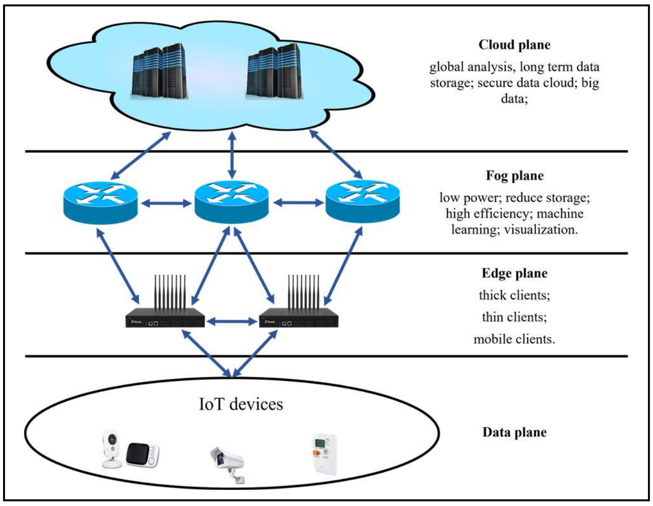
Cloud plane
global analysis, long term data storage; secure data cloud; big data;
Fog plane
low power; reduce storage; high efficiency; machine learning; visualization.
Edge plane
thick clients;
thin clients;
mobile clients.
IoT devices
Data plane

Fig. 1. The main connection of cryptography in Cloud of Things [2]

Edge computing is a set of technical solutions that allow computation to be performed at the network's edge. They consist of computing and network resources located between cloud data centres and the devices producing or collecting the data. The basic principle of Edge Computing is that the necessary computations must be performed close to the data sources, where all information coming from the source devices is analysed and evaluated. Accordingly, it is an excellent application for IoT systems, where computing resources located near IoT devices can perform these analyses so that only the "useful" information is uploaded to the cloud.

Fog Computing is a layered model for providing access to scalable computing resources continuously. It can be used to facilitate the deployment of distributed and/or latencysensitive applications and services. It is structured as physical or virtual fog nodes between cloud services and network-connected end devices (smart devices, IoT elements). Nodes are network devices such as routers, switches, gateways, and hubs that can contribute to the high throughput of the network, thus supporting the centralisation of data centres, i.e., Cloud Computing. Fog nodes act as middleware and extensible services and support two-way communication and data management, ensuring continuous access to stored and processed data. Fog computing provides Quality of Service (QoS) for common cloud services such as low latency, data protection and security, and low power consumption. These form the basis for smart cities, including smart healthcare, smart homes, smart transport, and smart manufacturing.

Based on the above, Edge Computing can be equated to a network layer that provides local computing capacity to users and end devices located there, such as smart devices in the home or industry, smart city end devices, or other devices with networking capabilities. The essence of Fog Computing is that hardware and software functions are decoupled in a multi-layer architecture, allowing the applications to be dynamically transformed. It also provides computing and transferring services, except that it does this physically elsewhere, appearing only as a virtual service at the end devices. In contrast to Edge Computing, Fog Computing deals with the storage, control, and acceleration of data processing in addition to computing and networking [3].

The review of the relevant literature reveals that a significant number of the related keywords for Edge Computing and Fog Computing are connected to security, network security and information privacy.

A. *Threats and vulnerabilities in Cloud of Things*

In the next phase of the research, vulnerabilities and threats to the Cloud of Things were identified. For this, the author used the issues identified in the article by A. A. Abba Ari et al. published in 2019, which are presented in the Table II:

TABLE II. SECURITY AND PRIVACY THREATS ON CLOUD OF THINGS [4]

Security threats				
Communication threats	Physical threats	Data threats	Service provisioning threats	Other threats
Denial of Service	Device capture	Threats during retrieval from devices, transfer, and storage	Unidentified and unauthorized access	Malicious insiders
Eavesdropping	Node damaging	Deployment of unauthorized device	Identity theft	Shared technology issues
Spoof attack	Side channel attack	Key compromization and the breakage of cryptographic protocols	Service hijacking	Abusing cloud computing
Man-in-the-middle attack		False data injection	Insecure or compromising interfaces and API	
Replay attack		Data loss and leakage		
		Data breaches		
Privacy threats				
Vulnerabilities in web applications	Unnoticed capture and unaware identification	Lacking breach response	Lack of control and transparency	Unauthorized disclosure and loss of governance
Profiling and tracking	Unforeseen inference	Outdated or incorrect personal data		

In response to these threats, the author has begun examining the relevant literature published in 2020 and 2021 to see how they have changed in the view of experts researching and publishing on the subject in the recent period. Accordingly, the most frequently mentioned vulnerabilities and risks were examined, and the terms most often associated with them. From the results, the ten most frequently appearing terms were selected and collected in the table below.

TABLE III. THE TOP 10 THREATS AND VULNERABILITIES IN CLOUD OF THINGS

Threats and vulnerabilities	Most related terms
botnet	5g, coordinated attack, denial-of-service attack, honeypots, malicious activities, malware spread, network attack
bugs	cloud computing security, cloud network security, computer bugs, logic bugs, program vulnerability
denial-of-service attack	botnet attack, communication security, data security, malware, network security, security risk analysis, security systems
firmware	dark web, DDoS attack, security attacks, supply chain risk, system vulnerabilities
malware	denial-of-service attack, malicious activities, malicious injection attack, network security, security vulnerabilities, zero knowledge
man-in-the-middle attack	delay, eavesdropping, end-to-end security, known key attacks, malicious activities, network security, security problems
security and privacy issues	big data, data loss, data manipulation, privacy leakage, unauthorized access
side channel attack	cloud computing security, cybercrime, datamining, firewall security, single point failure
spoofing attacks	ARP attack, data stealing, denial-of-service attack, flooding attack, IP spoofing, malicious injection attack, virus infection
unauthorized access	access control, authorization, breaches, collusion attack, privacy leakage

For the most common threats, correlations can be identified. Accordingly, it can be declared that, for example, spoofing and flooding attacks can result from malicious injection attacks (malware) leading to a denial of service, which can be caused by a known firmware bug that has not been fixed by the manufacturer or by the user not keeping their device up to date (using outdated firmware).

B. Security solutions in Cloud of Things

The next part of the research aimed to identify the best protection solutions. Therefore, the author has searched for the terms that best reflect the security solutions applied to preserve data and maintain adequate security in the Cloud of Things. After the visualisation, comparison, and analysis, the following security solutions were identified:

- access control;
- authentication;
- cryptography;
- intrusion detection;
- key management;
- network security;
- secure transmission;
- security of data;
- security policy;
- software update.

The relationship between them was also perfectly identifiable. To illustrate this, the author used the VOSViewer software so that in Fig. 1, all the relevant keywords and phrases related to the term cryptography are well visible.

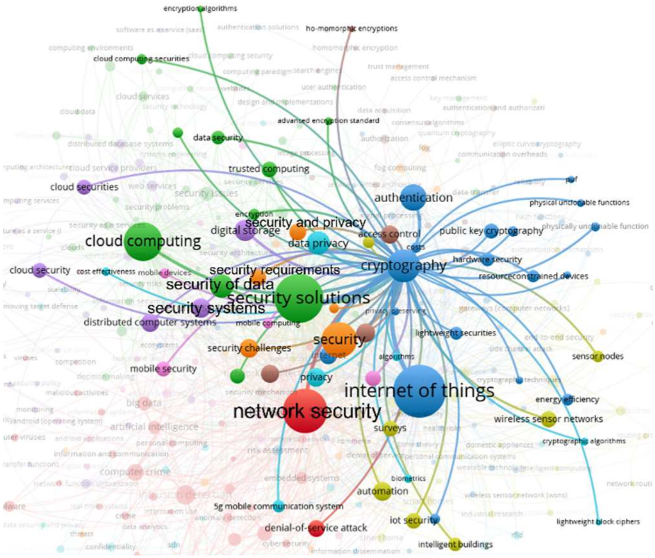

Fig. 2. The main connection of cryptography in Cloud of Things

VI. Results

As stated above, there is a strong correlation between the different risks and vulnerabilities. One of the most frequently used terms when examining threats was the botnet. The reason is that botnets can affect both IoTs and cloud services seriously. Botnets are a collection of infected end devices that execute malicious tasks based on instructions. Accordingly, the most common forms of attacks with botnets are:

- distributed denial of service;
- click fraud;
- phishing extortion;
- key logging;
- bitcoins misrepresentation;
- spamming
- sniffing traffic;
- malware spreading;
- secret word stealer;
- mass extensive fraud with bots [5].

As with IoT and cloud services, one of the biggest threats and challenges for the Cloud of Things is the denial of service, where an attacker makes various services unavailable and systems unusable, usually with botnets. This is usually achieved by flooding the target with continuous ping packets to eventually be unable to respond to the large number of requests coming its way and stop functioning. However, this type of attack is not only capable of shutting down the service completely but also provides an excellent opportunity for IP spoofing attacks. The biggest problem with spoofing is that it is very difficult to identify the malicious attackers, so they can subsequently spread malicious code across the network almost unhindered, for example [6].

A. M. Abdelrahman et al. identified the threats that can occur at different layers in software-defined networks in [7]. These network solutions are usually applied to cloud computing, including Cloud of Things. The vulnerabilities in each layer, such as data, control, management, and application, have been defined, as shown in Fig. 2.

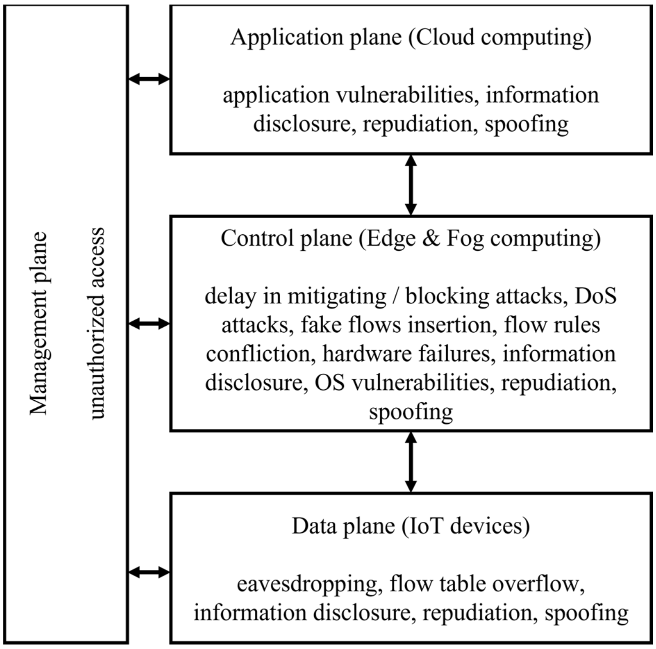
Management plane
unauthorized access
Application plane (Cloud computing)
application vulnerabilities, information disclosure, repudiation, spoofing
Control plane (Edge & Fog computing)
delay in mitigating / blocking attacks, DoS attacks, fake flows insertion, flow rules confliction, hardware failures, information disclosure, OS vulnerabilities, repudiation, spoofing
Data plane (IoT devices)
eavesdropping, flow table overflow, information disclosure, repudiation, spoofing

Fig. 3. Security threats in software-defined networking Cloud of Things [7]

From the threats identified here, the links can also be identified as in the overall analysis above. The issues at each plane, in most cases, mutually reinforce each other, which is why it is necessary to develop appropriate protection at each layer.

The priority is to protect IoT devices and networks at the data layer, which requires tools and software that help prevent, for example, man-in-the-middle attacks, thus avoiding eavesdropping and unauthorized access. Avoiding the possibility of data modification is also important, and appropriate measures must be taken to counteract this. The following procedures, among others, can contribute to this:

- access control;
- authentication;
- authorization;
- countermeasures for malicious hardware/software injection;
- cryptographic schemes;
- decentralization;
- intrusion detection system;
- policy-based mechanisms;
- prior testing;
- reliable routing protocols;
- secure data analysis;
- securing firmware update [8].

To increase the security of IoT systems, services can be installed at the edge layer to ensure adequate protection at the control plane. Services placed here can include the security profile manager, security analysis, protocol mapping, a security simulation, communication interface management, and request handling. In addition, solutions that support key management, authentication, authorisation, and accounting functions and appropriate access control may be included. Their implementation will release resources in IoT systems, for example, reducing the load on their computing capacity. Edge computing can also help to provide end-to-end security. Middleware elements can be implemented to provide a secure communication channel between endpoints, whether they are directly in the IoT network or the cloud. There are also several advantages to placing firewalls on the perimeter. The first is that firewall management is significantly easier as there is only one central firewall. Update tasks are also easier to perform. In addition, through this device, the management of IoT subsystems can be easily implemented to adapt to the security needs of the subsystem. It also has the added benefit of supporting mobile device tracking, meaning that if a device or user is on the move, it can be continuously connected to the central firewall with its credentials, keeping the data protected. The intrusion detection systems installed here, like firewalls, can continuously monitor the entire IoT network to identify a potential attack [9].

Processes in the fog plane must be defined to ensure secure information sharing between endpoints and cloud-based storage and application servers. The placement of traffic flow analysers in the fog layer contributes to the continuous monitoring of the communication taking place there. By monitoring the sending and receiving of data, they can check the frequency with which packets are sent, thus preventing, for example, a DDoS attack. They can also look for known patterns of malicious data, preventing malicious packets from being sent from blacklisted IP addresses, and add TCP flooding patterns to identify attacks and malicious behaviours across the network. Traffic flow classification solutions help speed up data processing by ensuring that the system only processes valuable data. Malicious traffic can also be filtered during the classification process, making the services even more secure. Service management supports fog infrastructure and services based on dynamic and distributed policies. These solutions can also filter specific threat patterns to prevent a potential attack [10]. A fog-based security model can provide the encryption processes between layers (data, application) to ensure a high level of security for IoT data processed and stored in the cloud. The model can also offer security properties, including access control, authentication, privacy and data protection, and security profile [11].

Implemented procedures in the cloud are also essential to ensure the security of the data and applications running in the cloud and protect them from unauthorised access, modification, and leakage. To protect data, a secure, scalable, and flexible access control method is essential, in which users are assigned attributes and access to data is determined based on the user's attribute. Mandatory authentication and authorisation checks should be defined for all users before accessing data and services stored in the cloud. Users who no longer need access to data and services should have their access withdrawn as soon as possible to prevent unauthorised access, so appropriate access management must be put in place. Data segregation or data classification techniques allow data to be separated based on its sensitivity, which can not only prevent unauthorised access but also help to ensure proper use of storage capacity. Encryption is essential for secure storage and transport. The first element of the CIA principle of information security is also provided with it, i.e., confidentiality is sustainable as only a person with the right key can unlock the encryption and access the data. To maintain data integrity stored in the cloud, data should be regularly checked for unauthorised modifications, tampering or leaks. In the cloud, high availability of data can be ensured through replication or redundancy, backing up data in different geographical locations. A strong focus should be placed on securing the application programming interfaces (API) used to guarantee application security. APIs act as an intersection between cloud services and cloud applications, and therefore they are particularly vulnerable to the data they handle. All input data must be validated before being used by the service to prevent data loss, spoofing or flooding attacks. To ensure access, the authorisation and authentication of each service request must be checked. To increase the security and availability of data and services, automated applications can backup, patch, and monitor applications. The status of applications can be backed up periodically to ensure higher availability, which can also be useful when restoring data and services. Applications can also be developed to automate updates, providing secure update services and management [12].

Following the keyword analysis, a deeper analysis of the relevant literature identified the security solutions most typical for each layer of the Cloud of Things, which are illustrated in Fig. 3.

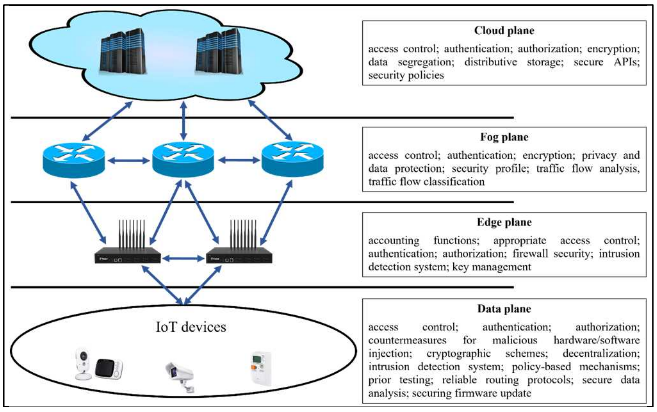
Cloud plane
access control; authentication; authorization; encryption; data segregation; distributive storage; secure APIs; security policies
Fog plane
access control; authentication; encryption; privacy and data protection; security profile; traffic flow analysis, traffic flow classification
Edge plane
accounting functions; appropriate access control; authentication; authorization; firewall security; intrusion detection system; key management
Data plane
access control; authentication; authorization; countermeasures for malicious hardware/software injection; cryptographic schemes; decentralization; intrusion detection system; policy-based mechanisms; prior testing; reliable routing protocols; secure data analysis; securing firmware update
IoT devices

Fig. 4. Security solutions in Cloud of Things

VII. Conclusion and Future Scope

In this article, the author has used keyword analysis to answer the questions of the most significant security challenges in the Cloud of Things and what security solutions can be applied at the data, edge, fog, and cloud layers. After a keyword analysis, he was able to answer these questions and identify the best practices that can contribute to the cloud-based protection of IoT devices.

The results will be used in the other phases of the research, where the author will continue to analyse the possibilities of combining IoT devices and cloud computing. The above research was the second step of a larger study, after which the author will examine the potential of using cloud-based IoT services in the defence sector, such as the military, police, and public administration.

Literature Used for the Analysis

A. Al-Qerem, M. Alauthman, A. Almomani, and B. B. Gupta: "IoT transaction processing through cooperative concurrency control on fog–cloud computing environment", Soft Computing, vol. 24, no. 8, pp. 5695–5711, 2020, doi: 10.1007/s00500-019-04220-y.

A. Kallel, M. Rekik, and M. Khemakhem: "IoT-fog-cloud based architecture for smart systems: Prototypes of autism and COVID-19 monitoring systems", Software - Practice and Experience, vol. 51, no. 1, pp. 91–116, 2021, doi: 10.1002/spe.2924.

D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang: "'Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach", IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6143–6149, 2020, doi: 10.1109/JIOT.2020.2977196.

L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider: "IoT privacy and security: Challenges and solutions", Applied Sciences (Switzerland), vol. 10, no. 12, 2020, doi: 10.3390/APP10124102.

L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong: "Edge-Computing-Enabled Smart Cities: A Comprehensive Survey", IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10200–10232, 2020, doi: 10.1109/JIOT.2020.2987070.

M. Abbasi, E. Mohammadi-Pasand, and M. R. Khosravi: "Intelligent workload allocation in IoT–Fog–cloud architecture towards mobile edge computing", Computer Communications, vol. 169, pp. 71–80, 2021, doi: 10.1016/j.comcom.2021.01.022.

M. Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos: "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment", Journal of Network and Computer Applications, vol. 150, 2020, doi: 10.1016/j.jnca.2019.102496.

Q. Fan and N. Ansari: "Towards Workload Balancing in Fog Computing Empowered IoT", IEEE Transactions on Network Science and Engineering, vol. 7, no. 1, pp. 253–262, 2020, doi: 10.1109/TNSE.2018.2852762.

S. A. Hashmi, C. F. Ali, and S. Zafar: "Internet of things and cloud computing-based energy management system for demand side management in smart grid", International Journal of Energy Research, vol. 45, no. 1, pp. 1007–1022, 2021, doi: 10.1002/er.6141.

S. Tuli et al.: "HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments", Future Generation Computer Systems, vol. 104, pp. 187–200, 2020, doi: 10.1016/j.future.2019.10.043.

T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie: "MTES: An Intelligent Trust Evaluation Scheme in Sensor-Cloud-Enabled Industrial Internet of Things", IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2054–2062, 2020, doi: 10.1109/TII.2019.2930286.

W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah: "Industrial internet of things: Recent advances, enabling technologies and open challenges", Computers and Electrical Engineering, vol. 81, 2020, doi: 10.1016/j.compeleceng.2019.106522.

W.-Z. Zhang et al.: "Secure and Optimized Load Balancing for Multitier IoT and Edge-Cloud Computing Systems", IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8119–8132, 2021, doi: 10.1109/JIOT.2020.3042433.

Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen: "Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things", IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6722–6747, 2020, doi: 10.1109/JIOT.2020.3004500.

Z. Lv and W. Xiu: "Interaction of Edge-Cloud Computing Based on SDN and NFV for Next Generation IoT", IEEE Internet of Things Journal, vol. 7, no. 7, pp. 5706–5712, 2020, doi: 10.1109/JIOT.2019.2942719.

References

[1] R. Geetha, A. K. Suntheya, and G. U. Srikanth: "Cloud Integrated IoT Enabled Sensor Network Security: Research Issues and Solutions", Wireless Personal Communications, vol. 113, no. 2, pp. 747–771, 2020, doi: 10.1007/s11277-020-07251-z

[2] F. Mehmood, I. Ullah, S. Ahmad, and D.-H. Kim: "A novel approach towards the design and implementation of virtual network based on controller in future iot applications", Electronics (Switzerland), vol. 9, no. 4, 2020, doi: 10.3390/electronics9040604.

[3] M. Iorga, L. Feldman, R. Barton, M.J. Martin, N. Goren, C. Mahmoudi: "Fog computing conceptual model", (NIST SP 500-325), available from: https://doi.org/10.6028/NIST.SP.500-325, accessed 05 May 2021.

[4] A. Abba Ari, O. Ngangmo, C. Titouna, O. Thiare, Kolyang, A. Mohamadou, A.M. Gueroui: „Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges", Applied Computing and Informatics, Jan. 2020, ISSN: 2210-8327, doi: 10.1016/j.aci.2019.11.005

[5] S. Nagendra Prabhu, D. Shanthi Saravanan, V. Chandrasekar, and S. Shanthi, "Recognition of botnet by examining link failures in cloud network by exhausting canfes classifier approach", Advances in Intelligent Systems and Computing, vol. 1171, pp. 179–189, 2021, doi: 10.1007/978-981-15-5400-1_18

[6] V. Singh and S. K. Pandey, "Revisiting Cloud Security Threats: IP Spoofing", Advances in Intelligent Systems and Computing, vol. 1053, pp. 225–236, 2020, doi: 10.1007/978-981-15-0751-9_21

[7] A.M. Abdelrahman, J.J.P.C. Rodrigues, M.M.E. Mahmoud, K. Saleem, A.K. Das, V. Korotaev, and S.A. Kozlov: „Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions", International Journal of Communication Systems, vol. 34, no. 4, 2021, doi: 10.1002/dac.4706

[8] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things", IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4004–4022, 2021, doi: 10.1109/JIOT.2020.3015432

[9] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security", Digital Communications and Networks, vol. 6, no. 2, pp. 195–202, 2020, doi: 10.1016/j.dcan.2019.08.006

[10] S. Rathore, J. H. Park, and H. Chang, "Deep Learning and Blockchain-empowered Security Framework for Intelligent 5G-enabled IoT", IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3077069

[11] A. A. Sadri, A. M. Rahmani, M. Saberikamarposhti, and M. Hosseinzadeh, "Fog data management: A vision, challenges, and future directions", Journal of Network and Computer Applications, vol. 174, 2021, doi: 10.1016/j.jnca.2020.102882

[12] S. S. Manakattu, S. Murugesh, and R. N. Hirekurabar, "Security Landscape for Private Cloud", Lecture Notes in Networks and Systems, vol. 98, pp. 67–78, 2020, doi: 10.1007/978-3-030-33846-6_8