https://doi.org/10.46335/IJIES.2024.9.6.22 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 107-114

International Journal of Innovations in Engineering and Science, www.ijies.net

A Comprehensive Review of IoT Security and Privacy Challenges in Cloud-Based Systems

Ranjan Kumar Gupta[1], Dr. Ranu Pandey[2]

[1]*Research Scholar, Department of Computer Science, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India*
[1]*kumarranjange@gmail.com*
[2]*Assistant Professor, Department of Computer Science, Shri Rawatpura Sarkar University, Raipur Chhattisgarh, India*
[2]*ranu_pandey8@hotmail.com*

***Received on**: 5 May,2024* ***Revised on**: 30 June,2024* ***Published on**: 02 July ,2024*

***Abstract** – Cloud computing in conjunction with the Internet of Things (IoT) has transformed the industries through the ability to provide high-levels of scalability, efficiency, and automation previously unattainable. Nevertheless, since all IoT devices gather and transfer sensitive information over networks, one of the most recent challenges that have been encountered is privacy and security issues. This review paper discusses the serious concerns associated with the security and privacy of the IoT-cloud based systems and in specific, the frameworks such as General Data Protection Regulation (GDPR) and Privacy by Design (PbD). Such frameworks are necessary to guarantee that the management of the aspects of privacy is embedded within the entire scheme of system lifecycle such as information gathering, storage and communication. The article addresses the multidimensional requirements of privacy, comprising data minimized, transparency and accountability and how secure communication protocol and robust encryption technique can help reduce security risks. The paper further discusses authentication schemes, access control and the process of having to find the balance around security and the demand to have uninterrupted systems in an IoT. This has raised the complexity of IoT networks, and more procedures of privacy protection are required to be updated in response to the new threats. Integrating secure systems, active privacy policies, and sound cryptographic algorithms, the IoT-cloud-based systems can become safe, expandable, and privacy-sensitive tools covering a broad range of applications to guarantee the security of the sensitive data of the users.*

***Keywords**- DDoS Attacks, General Data Protection Regulation (GDPR), IoT-cloud-based systems, Privacy by Design (PbD)*

INTRODUCTION

The combination of the Internet of Things (IoT) and cloud computing has revolutionized industries in a way that introduced new levels of convenience, effectiveness and scalability. IoT can also streamline operations in the industries like smart cities, healthcare, manufacturing and agriculture by making devices talk to each other and connect effortlessly over large distances. Nevertheless, such a change has brought with it great issues of data security and privacy. With the advancement in the number of IoT devices, sensitive data (personal health information, financial information, and location information) are gathered, data-mined, and shared, exposing them to an enhanced probability of falling under possible cyberattacks.

As cloud computing continues to be used as a storage and processing option when it comes to IoT data, the importance of effective security and privacy infrastructure cannot be more essential. With the emergence of the IoT and cloud computing, there is also the introduction of new challenges of providing confidentiality, integrity, and availability of the data when conventional security mechanisms are not sufficient in coping with dynamic threats. A major issue of concern was how data can be easily tampered with, stolen, and hacked especially during cloud-based systems where highly sensitive data are stored and transferred over various devices and networks.

https://doi.org/10.46335/IJIES.2024.9.6.22 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 107-114

The paper represents the overview of the security parameters and privacy reports of IoT-cloud-based framework. It discusses some of the major models of privacy that are currently defining the functionality of the secure and privacy-sensitive IoT frameworks, including General Data Protection Regulation (GDPR), Privacy by Design (PbD). In addition, it presents fundamental issues of IoT security like data lifecycle protection, data authentication procedures, and encryption methods and also suggests how personal and sensitive data could be safeguarded. IoT-cloud systems can achieve internet security reliability into the future by incorporating the best privacy protection strategies and using secure communication standards in order to facilitate the further development of IoT technologies with the issue of privacy not lost.

SECURITY IN COMMUNICATION NETWORKS

2.1 Basic Issues

Since polling places may be dispersed, as far as establishing security is concerned, it is of great importance that communication systems are designed to integrate them with:

- The combined operations center (see Operations and Security Centers) or the electoral and security operations centers in distinct systems;
- The bases of security forces operation;
- Any mobile security unit (see Rapid Reaction and Reserve Forces)

This necessitates that every polling site should be connected to the good communications network. Choosing between the kind of network to be adopted in the event of high-risk occasions, the reliability concerns in this critical sector of logistics should outweigh the cost factor considerations. In low-risk cases, this can just be affording the available telephone lines [1].

2.2 Uses of Telecommunications

It is not just necessary to have a reliable telecommunications system on election day but is also vital in normal operating with regard to the following points:

- Consult the advice of a legal or operational problem;
- Report the polling place activity on regular basis;
- Alert election administrators on the requirement of any other supplies and emergency staff;
- Report on the easy commencement and ending of voting;
- Declaration of the transmission of any electoral contents;
- Notify of provisional outcomes (in case the scrutiny is done polling places).

The fact that communications are received and used multiple times is a good deciding factor to have both security and operational concerns in polling locations handled in a joint operations center where one system can utilize the channels previously acquired in the same fashion [2].

2.3 Planning Issues

The necessity in communication may place restriction on the location of the polling stations. In case radios or mobile phones are to be utilized, locating the polling station in shady spots (i.e., in the buildings or those zones that get or receive signaling poorly) will make the communication strategy a failure. Prior to using any communications system, it must go through stringent tests to determine whether it will work in all the regions where it will be implemented particularly where there will be usage of telephones or portable radios [3].

System loading also needs to be estimated in order to determine communication strategies. The load factors may be transformed into too central communications systems that are not so reliable. In the event that portable equipment is required, the layout plans must allow adequate time to enable all the individuals involved to get the necessary training to accustom themselves to the use of the equipment before utilizing it [4].

2.4 Communication Arrangements

The lowest acceptable standard in environments of low risks is the access to the telephone communication system with each polling place being able to access one within the precinct itself, either fixed or mobile. In low-risk situations however, access to telephone line in the neighbourhood might be adequate provided access is guaranteed all through the duration of operation at the polling stations. In remote locations, one should provide radio communication in each voting place and should make use of existing facilities.

In more risky situations, a more efficient process than the telephone that can in real time connect with traveling

https://doi.org/10.46335/IJIES.2024.9.6.22 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 107-114

security units is usually needed. Typically, this means finding the most suitable formulas to initiate radio communications with all the polling stations, in the cost-effectiveness terms. Mounting on already existing radio network will obviously be more economical, but cost of equipping each of the polling places with radio equipment will still be high unless they can be borrowed.

Utilization of many different networks (such as military and police) should most of the time be avoided, with the exception of geographical coverage motives. When all the sites are linked through the same format it becomes less confusing. Telecommunications systems belonging to the security forces may offer the most effective, reliable services and covering a maximum land area provided it can be ascertained that it would be able to deliver a professional service. It is also beneficial in the fact that it might be a name that is already known by many who would require using it.

2.5 Communication Procedures

Telecommunication cannot be effective without common procedures and these procedures ought to have methods and ways of communication. Poll volunteers ought to possess a recent list of the mobile phones or radio frequencies of all voting places, voter supervision offices and security agencies. The security groups and voting officers should possess fresh copies of the information.

The introduction of a routine in the news provision at the polling station and security teams will support the goals of information and security. In the case of using the personal radios, the location frequencies should be rationally planned and managed. The radio or telephone report should have formats to be defined with the aim of:

- Enable a quick identification of the issuer;
- Facilitate passage of information in a transparent way;
- The emergencies should be given first priority;
- Prevent congestion in the network (line congestion).

Communications made through radio and personal telephone should also be sufficient with a number of personnel at the reception bases to ensure that every call could be answered within the time the polling stations are operational. This is to be incorporated with time when material will be moved in and out of the polling stations. Training of voting officers, administrative staffs, and security forces should be provided with the application of telecommunications networks and equipment.

PREVENTION OF DDOS ATTACKS

In particular denial-of-service attacks, particularly by botnets, are hard to prevent, or even detect, and yet it is also possible based on the same principles as it is possible with any other attack:

3.1 Monitoring and Knowledge of the Platform

Despite the lack of innovativeness, the knowledge about the service provided is required in order to be capable of undertaking the task of preventing the attacks, and, in most of the cases, the information appears, yet in the disjointed form (typically, due to the fact that it is stored in the "departments"), when the overview and awareness of the platform should be global so that to make a best use of it. The following aspects ought to be taken into account [5]:

1. Typical service behaviour, which would include number of new requests based on the time line, location of the clients accessing the service, ports and required connection flows, bandwidth utilized, average values of CPU, memory, etc. of devices so that they can be compared in the case of attacks or anomalous behaviours.
2. Maximum limits to which all devices subjected can be run along with the operating limits considering other services in case of shared devices (servers, firewalls, balancers, routers, etc.) to identify the potential bottlenecks of the service in advance.

The anticipated capacities with the duration and new services that could influence the information of the two aforementioned points. The majority of the background information is received through an accurate tracking of the platform hence this survey would serve a dual purpose; on the one hand to gather the data about the points mentioned above and on the other hand to gather and process information to understand that it is under attack and on the other hand to stop it as would be seen in the next section on detection and mitigation [6].

The information gathered by the surveillance mechanisms ought to be processed beyond the review in a case of a major attack. Periodic searches are advisable to find the sources of small attacks, which might even have not been noticed, or to find abnormal behavior of service that could be the source of further issues [7].

https://doi.org/10.46335/IJIES.2024.9.6.22 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 107-114

To perform full monitoring, encrypted traffic should also be examined, as increasing numbers of DoS attacks have now switched to use encrypted protocols like SSL to make their attacks more opacity like, as in most instances the traffic is not decrypted in order that it may be monitored and this creates performance dilemma besides the legal issues which are brought in by declassifying the information it carries [8].

3.2 Correct Design of the Platform and Planning of Procedures

Without the information connected with the above point, it is impossible to develop a good service architecture design. The statistics on the typical operation of the service and the forecast of the growth are vital as far as correct dimensioning is concerned, the topology planning, and selecting the devices that the service platform comprises [9].

Sometimes, a given correction factor can be introduced during equipment sizing, to enable the architecture to handle a rather higher level of load, as compared with the typical maximums (and expected growth), that is less subject to attacks.

Another suggestion is to put in place items that are specifically meant to tutor parts of the service, such that the majority of the connectivity is directed to these items without any need to get the demands to the backend server.

It may be said that the measures are effective scenarios; they are however, scenarios that imply an extra cost or rather oversizing nearly all situations are overly costly to factor into the decision [10].

The other aspect which is worth attention in the design in terms of DoS attack prevention is the suspension of capabilities that are unutilized or can possibly be used as an attack avenue. Here, it may include some of the existing examples already given above like in deactivating the monlist command in NTP servers, or in recursion domain servers. Such functionalities may not only be limited to servers, but also any elements of the network that can be at risk of being attacked, including routers (IP fragmentation, ICMP redirects, pings to broadcast addresses, STP attacks, etc.) [11].

Routers also have configurations that can stop DoS attacks e.g. disabling IP fragmentation. It is the setup in which we can be immune to attacks based on packing fragmentation, which either serve to skip firewalls and their anti-DoS traversal, or as an attack vector on its own sending multiple packets that must be reassembled consuming a huge amount of router CPU (where packets are sent through tunnel this problem is magnified) [12].

Similarly, where possible, it is wise to restrict the total number of connections and per unique user (typically per source IP), and the number of new connections per second (both globally, and, respectively, per single user). Likewise, session establishment and established sessions timers may sometimes be capped (to avoid letting sessions which are not used long time remaining in the memory table), the method being that many DoS attacks thrive on reducing the memory of the equipment by creating many connections of the kind known as half opened, that is, not completely, as they wait in the opening time slot (connection establishment slot). The equipment that receives opening request must use memory to hold the state of the half connection, waiting to get completed [13].

Timer configurations come in handy regarding prevention of the impact of attacks but it is necessary to consider that they are markedly subject to the services underlying it, such as there are database services that require the maintenance of connections so they can last without usage over a period of hours hence when the session timer is limited the connection may in turn get interrupted at intervals [14].

Conversely, besides the DoS settings, which limit the bandwidth usage, which is also useful to limit the effects of the DoS attack, another good idea, where possible, is to set maximum values of resources used by the applications, e.g. will the service is on a virtual machine, or the connections go through a physical firewall that has been split in several virtual ones, the maximum number of CPU cycles, memory and connections (in the case of the firewall) that it can demand from the host machine so that the attack on a given service does not affect others not under immediate attack [15].

To conclude, the following ideas on configurations that should be kept in mind have been brought up [16]:

- Restrict the maximum total number of connections and connections per user, restrictions on the number of new connections as a whole and per user.
- Enforce DoS policy on the traffic.
- In opening up on new connections, minimize session established and wait timers.

https://doi.org/10.46335/IJIES.2024.9.6.22 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 107-114

- Minimize the exploitation of resources (CPU, memory, network and disk) used on shared or virtualized systems.

The security architecture forms an important component of the design with regard to DoS and DDoS prevention. This should in any case provide antispoofing policies (which should also be implemented in the routers using the configuration of URPF, where BGP is used), and limit access to client IPs, where this is possible, e.g., It is possible that an NTP service is offered; then only self-administered IPs should be allowed to issue requests of this kind, and certainly they cannot be offered to the entire world, as it will allow an intruder (whose IP will not be under our administration) to take advantage of a documented vulnerability [17].

Conversely, application control and security features, e.g., layer 7 firewalls, IPS and others become more and more significant as way to both reduce DoS attacks based on the exploits/software faults of the applications at hand, and actively to clear the connections that are simply badly crafted [18].

To conclude the security section, it is sufficient to mention that, once again, we will have to work with antivirus and antimalware, so that servers and PCs could not be a part of botnet that will attack third parties or oneself.

Another issue that is common with respect to mitigation of DoS and DDoS attacks is that, in most of the instances, measures undertaken to mitigate them are not beneficial to the actions not similarly undertaken by other parts of the world. To take an example; the fact that they, through their own NTP servers, cannot utilize monlist is not the reason why it cannot be facilitated by another NTP server in another administration and hence can be attacked by the said other NTP server to affect an attack on their own service.

After the design and security indications have been observed, just one more should be stressed, which is that much of the prevention (and mitigation as will subsequently be observed) may be implemented by a third party, or even by the actual ISP providing the connection and therefore it is important to plan with them the possibility of utilizing such added services in case of contingency or even on a continuous basis [19].

One of the considerations that may be considered as part of prevention includes the planning of the action to be taken in case of contingency, the examination of how tasks could be automated in the event of attack detection and the application of counter measure to ensure the attack could be detected and stopped before causing damages to the service [19].

3.3 Auditing and Remediation of Vulnerabilities

The remaining prevention strategy would be periodic conductance of audits with the aim of revealing and rectifying the weaknesses of the service. During such audits, the bottleneck location (not only network one) and configuration failures are to be re-examined. The response of the platform against stress will also be subjected to load tests. Similarly, it must be determined whether it is safe against the most recent known vulnerabilities and attacks by updating items such as applications and Operating Systems when required [20].

PRIVACY REQUIREMENTS IN IOT-CLOUD-BASED SYSTEMS

Demanding the privacy of the IoT-based systems on cloud systems is a complex-like issue that considers volumes of personal, medical, and financial data which IoT devices typically produce. The privacy requirements are supposed to encompass the entire process of data management including its destruction in the end. General Data Protection Regulation (GDPR) has become an important framework on personal data protection, and this has impacted on the designing aspects of privacy policies concerning those of the IoT-cloud systems around the world. It focuses on the principles such as data minimization, transparency, and accountability, which are highly necessary in order to win user trust.

Also, the idea of Privacy by Design (PbD) has gained centrality in designing systems that are safe. PbD promotes privacy requirements at the very early stages of system design and architecture as opposed to adding privacy features post development. The framework puts stress on proactive actions to safeguard privacy in respect to the brief of the system. According to studies conducted by [21], [22], and [23], there has been the development of PbD as a conceptual framework and an engineering approach that enables privacy risks by establishing mitigation measures in the process of system development.

Moreover, the privacy protection measures applied to the IoT-cloud based systems may include such approaches as cloud computing, data anonymization, change tracking, and sophisticated analytics. All these methods assist in making the data secure during its receipt and the

https://doi.org/10.46335/IJIES.2024.9.6.22 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 107-114

time it is stored in the cloud servers. The main difficulty is to apply these safety measures of privacy to individual aspects of a given system, in particular given the various services offered, including AI-driven diagnosis, active monitoring, and preventive care.

KEY SECURITY AND PRIVACY CHALLENGES IN IOT

As it is inherent to IoT devices, they are extremely distributed and interconnected and, therefore, at high risk of being subjected to several types of cyberattacks. The devices tend to perform on very low computational bites which in turn makes robust security procedures quite hard to incorporate. The issues related to the security of IoT are not only technical but also organizational because protection of the user's data involves the collaboration of efforts involving several parties.

Data lifecycle is one of the critical aspects in the security of IoT. It is also imperative to secure the data at all stages of its lifespan, including time of its creation, during its storage, its transport, and to the time it is deleted. IoT systems running on the cloud require strong mechanisms to facilitate the management of data throughout its lifecycle such as safe data archiving, effective transportation of the data and safe guided erasure protocols.

The other dilemma is making it fully functional as well as guaranteeing privacy and security. The work of IoT systems requires the balancing of the requirements in the continuity and convenience of work with the necessity of data protection. According to the researchers, the key to achieving both of the goals is shown in positive-sum configurations where the balance is reached between privacy and security without negative compromise to either. This necessitates the design of systems that are well planned and take into consideration any aspect that may compromise privacy and pre-empt the security tactics.

In addition, location privacy has also been found as a very important concern particularly due to the increase in location-based services. It is also essential to protect the geographical information on users and unless proper privacy techniques are set in place, sensitive location information may leak, which can cause serious privacy violations.

AUTHENTICATION PROTOCOLS AND SECURITY MEASURES

In order to guarantee that information within IoT-clouds remains secure and only users that are allowed to have data will have access, powerful authentication mechanisms are essential. According to [24], this is because a potent approach to authentication is symmetric key cryptography integrated with asymmetric key cryptography. These procedures, which are backed by secure devices e.g. smartcards, guarantee that prior to gaining access to sensitive information, the identities of the users must be authenticated.

It cannot be overemphasized that sound encryption procedures in securing IoT-cloud communications are mandatory. Among the researchers who underscore the significance of applying encryption at the different levels of systems, including hardware, operating system, and application, there are [25] and [26]. Encryption helps to ensure that data security is handled not only in communication but also in the storage process to eliminate unauthorized access thereby guaranteeing good data integrity.

Besides encryption and authentication, access control mechanisms offer one of the most crucial functions in the protection of IoT. As revealed in [27] and [28], limiting access rights of various users and ensuring important information can only be accessed by the relevant staff members minimizes the possibility of internal and external attacks.

SYSTEM REQUIREMENTS FOR SECURE IOT-CLOUD INTEGRATION

Security enabling the IoT-cloud-based systems to operate require incorporation of an efficient access control, secure communications, and privacy protection. Permission-based systems like the systems suggested by the authors of [27] guarantee that only the people with rights may view the information, hence data exploitation and unlawful entrance are avoided.

The factors that promote secure communication involve the use of secure communications, such as end-to-end encryption and cryptographic techniques that are vital in ensuring protection of data as it is being sent to the recipients. In the absence of these, the IoT devices and cloud services would be subjected to data interception and exploitation. In addition, maintaining high levels of privacy protection among IoT devices through direct compliance with GDPR is one of the main purposes necessary to handle trust among users and stakeholders.

https://doi.org/10.46335/IJIES.2024.9.6.22 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 107-114

International Journal of Innovations in Engineering and Science, www.ijies.net

ARTIFICIAL INTELLIGENCE IN IOT-CLOUD-BASED SYSTEMS

The use of artificial intelligence has played a great role in the decision-making process in various fields. Discussing the field of IoT-cloud-based systems, AI is capable of processing a great amount of data to increase efficiency of the systems, identify patterns, and make better decisions. The information that AI derives is of various kinds, which offers conjectures to improve the functionality efficiencies.

The intelligence associated with AI can also be very useful in the networks which require monitoring of the processes and analysis of real-time information such as connected systems. Examples of such are as follows:

- *To the Researchers:* AI is used to collect data, through different sources, after which fragments of data are multiplied to obtain real time statistics and insights. This will help in simplification of systems and trends which may not be evident at a particular time by conducting manual analysis.
- *To the Users:* Individuals will have additional freedom to manipulate and visualize the data to a higher extent with AI. This trend is continuously getting larger because many people would prefer to have connected ones to track and monitor all the activities that occur daily and offer additional information about the functioning of the system and trends.
- *To the Professionals:* Using AI, what the professionals may know to guide, tell or help the users about day-to-day processes is disclosed. This enhances the fact that the venture is less labor intensive in order to concentrate more on high value addition activities.

The amount of data generated and collected is far much beyond the human capacity of collecting such data manually. AI algorithms save much time and efforts of human beings and, therefore, increase the efficiency of the system.

AI has facilitated the use of interconnected devices that have made it possible to monitor and analyze more things and people in order to be able to notice potential problems early enough and optimize suitable reaction in various systems.

CONCLUSION

The combination of IoT and cloud computing leads to some impressive possibilities as well as major security and privacy issues. With the rise of IoT devices and their increased functionality and number, the protection of the confidential data that the devices will collect is becoming imperative. The paper has discussed the privacy and security issues of an IoT-cloud-based environment and stressed the necessity to implement privacy frameworks e.g. GDPR and Privacy by Design (PbD) as well as their increased adoption as a way to make sure that the issue of privacy is incorporated positively into the architecture of the system. With the application of secure communication protocols, strong encryption algorithms, thorough authentication processes, the personal data of IoT systems is also more capable of resisting the variety of cyber threats.

Also, the primary issues identified in the paper were the management of data lifecycles, the use of security and usability balance, and location privacy in IoT networks. The introduction to the review also points out the necessity to consistently incorporate new security measures to meet new threats presented by rapidly developing security measures, such as quantum computing. The IoT security must be viewed as the whole, and legal and regulatory treatments should complement the strong technical measures to guarantee both long-term feasibility and maintain the trust of the users in the IoT application.

To sum up, it is clear that IoT-cloud systems have tremendous potential in terms of application to a great number of industries, yet they should be created and supported in terms of privacy and security enforced. The current research and development of new solutions in the fields of encryption, access control and privacy frameworks would be able to contribute to possible overcoming of the challenges and future optimization of the IoT systems allowing them to become more secure, scalable and privacy aware in the future.

REFERENCES

[1] *Li, Bin, Zesong Fei, Yan Zhang, and Mohsen Guizani. "Secure UAV communication networks over 5G." IEEE Wireless Communications 26, no. 5 (2019): 114-120.*

[2] *Sun, Qindong, Kai Lin, Chengxiang Si, Yanyue Xu, Shancang Li, and Prosanta Gope. "A secure and*

anonymous communicate scheme over the internet of things." ACM Transactions on Sensor Networks (TOSN) 18, no. 3 (2022): 1-21.

[3] *Makoni, Sinfree B. "Language planning, security, police communication and multilingualism in uniform: The case of South African Police Services." Language & Communication 57 (2017): 48-56.*

[4] *Mishra, Sakshi, Kate Anderson, Brian Miller, Kyle Boyer, and Adam Warren. "Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies." Applied Energy 264 (2024): 114726.*

[5] *Bechtel, Michael, and Heechul Yun. "Denial-of-service attacks on shared cache in multicore: Analysis and prevention." In 2019 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), pp. 357-367. IEEE, 2019.*

[6] *Singh, Jagdeep, and Sunny Behal. "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions." Computer Science Review 37 (2024): 100279.*

[7] *Kaur, Parneet, Manish Kumar, and Abhinav Bhandari. "A review of detection approaches for distributed denial of service attacks." Systems Science & Control Engineering 5, no. 1 (2017): 301-320.*

[8] *Boillat, Luc, Jan von der Assen, M. Franco, and C. Killer. "A Tool for Visualization and Analysis of Distributed Denial-of-Service (DDoS) Attacks." Communication Systems Group, Department of Informatics, Universität Zürich (2024).*

[9] *Lima Filho, Francisco Sales de, Frederico AF Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, and Luiz F. Silveira. "Smart detection: an online approach for DoS/DDoS attack detection using machine learning." Security and Communication Networks 2019 (2019): 1-15.*

[10] *Praseed, Amit, and P. Santhi Thilagam. "DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications." IEEE Communications Surveys & Tutorials 21, no. 1 (2018): 661-685.*

[11] *Ballmann, Bastian. Understanding Network Hacks: Attack and Defense with Python 3. Springer Nature, 2021.*

[12] *Chai, Tze Uei, Hock Guan Goh, Soung-Yue Liew, and Vasaki Ponnusamy. "Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory." Systems 11, no. 4 (2023): 211.*

[13] *Kumari, Pooja, and Ankit Kumar Jain. "A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures." Computers & Security (2023): 103096.*

[14] *Ibtissam, Kharchouf, Mahmoud S. Abdelrahman, Abdulmeen Alrashide, and Osama A. Mohammed. "Assessment of Protection Schemes and their Security under Denial of Service Attacks." In 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), pp. 1-6. IEEE, 2022.*

[15] *Virupakshar, Karan B., Manjunath Asundi, Kishor Channal, Pooja Shettar, Somashekar Patil, and D. G. Narayan. "Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud." Procedia Computer Science 167 (2024): 2297-2307.*

[16] *Bhardwaj, Akashdeep, and Sam Goundar. "Cloud computing security services to mitigate DDoS attacks." In Cloud computing security-concepts and practice. IntechOpen, 2024.*

[17] *Jiang, Weiyu, Bingyang Liu, Chuang Wang, and Xue Yang. "Security-Oriented Network Architecture." Security and Communication Networks 2021 (2021): 1-16.*

[18] *Kautish, Sandeep, A. Reyana, and Ankit Vidyarthi. "SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment." IEEE Transactions on Industrial Informatics 18, no. 9 (2022): 6455-6463.*

[19] *Khalaf, Bashar Ahmed, Salama A. Mostafa, Aida Mustapha, Mazin Abed Mohammed, and Wafaa Mustafa Abduallah. "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods." IEEE Access 7 (2019): 51691-51713.*

[20] *Horak, Tibor, Peter Strelec, Ladislav Huraj, Pavol Tanuska, Andrea Vaclavova, and Michal Kebisek. "The vulnerability of the production line using industrial IoT systems under DDoS attack." Electronics 10, no. 4 (2021): 381.*

[21] *Dhatterwal, J.S., Kaswan, K.S., Baliyan, A. and Jain, V., 2022. Integration of Cloud and IoT for Smart e-Healthcare. In Connected e-Health: Integrated IoT and Cloud Computing (pp. 1-31). Cham: Springer International Publishing.*

[22] *Alshammari, M. and Simpson, A., 2018, January. Privacy architectural strategies: an approach for achieving various levels of privacy protection. In Proceedings of the 2018 Workshop on Privacy in the Electronic Society (pp. 143-154).*

[23] *Nwachukwu, O.J. 2017. Privacy by Design. Master's Degree of Science in Telematics: Communication Networks and Networked in Telematics-Communication Networks; Norwegian University of Science and Technology: Trondheim, Norway.*

[24] *Yu, Y., Hu, L. and Chu, J., 2024. A secure authentication and key agreement scheme for IoT-based cloud computing environment. Symmetry, 12(1), p.150.*

[25] *SargIoTis, D. (2024). Data security and privacy: Protecting sensitive information. In Data governance: a guide (pp. 217-245). Cham: Springer Nature Switzerland.*

[26] *Farahsari, P.S., Farahzadi, A., Rezazadeh, J. and Bagheri, A., 2022. A survey on indoor positioning systems for IoT-based applications. IEEE Internet of Things Journal, 9(10), pp.7680-7699.*

[27] *Kaliya, N. and Hussain, M., 2017, April. Framework for privacy preservation in IoT through classification and access control mechanisms. In 2017 2nd International Conference for Convergence in Technology (I2CT) (pp. 430-434). IEEE.*

[28] *Caiza, J.C., Martín, Y.S., Guamán, D.S., Del Alamo, J.M. and Yelmo, J.C., 2019. Reusable elements for the systematic design of privacy-friendly information systems: A mapping study. IEEE Access, 7, pp.66512-66535.*