

## Cloud and internet-of-things secure integration along with security concerns

Arif Ullah<sup>1</sup>, Imane Laassar<sup>2</sup>, Canan Batur Şahin<sup>3</sup>, Ozlem Batur Dinle<sup>4</sup>, Hanane Aznaoui<sup>5</sup>

<sup>1</sup>Department of Computing, Riphah International University, Faisalabad, Pakistan

<sup>2</sup>Faculty of Computer Science, Université Ibn Tofail, Kenitra, Morocco

<sup>3</sup>Faculty of Engineering and Natural Sciences, Malatya Turgut Ozal University, Malatya, Turkey

<sup>4</sup>Faculty of Computer Engineering, Siirt University, Siirt, Turkey

<sup>5</sup>LAMAI Laboratory, Faculty of Sciences and Techniques, Cady Ayyad University, Marrakech, Morocco

### Article Info

#### Article history:

Received Oct 13, 2021

Revised Jun 10, 2022

Accepted Jul 21, 2022

#### Keywords:

Challenges

Cloud computing

Internet of things

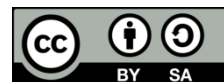
Security

Virtualization

### ABSTRACT

Cloud computing is a new technology which refers to an infrastructure where both software and hardware application are operate for the network with the help of internet. Cloud computing provide these services with the help of rule know as you pay as you go on. Internet of things (IoT) is a new technology which is growing rapidly in the field of telecommunications. The aim of IoT devices is to connect all things around us to the internet and thus provide us with smarter cities, intelligent homes and generally more comfortable lives. The combation of cloud computing and IoT devices make rapid development of both technologies. In this paper, we present information about IoT and cloud computing with a focus on the security issues of both technologies. Concluding we present the contribution of cloud computing to the IoT technology. Thus, it shows how the cloud computing technology improves the function of the IoT. Finally present the security challenges of both technologies IoT and cloud computing.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Arif Ullah

Department of Computing, Riphah International University

Faisalabad, Pakistan

Email: arifullah@riphahfsd.edu.pk

## 1. INTRODUCTION

Cloud computing is a contemporary technology which gives convenient to on-demand network access for sharing and pooling of resources on the network like storage servers and different application services for both application and hardware. The application serves as facilities on the internet with the hardware and system software work in the data centers for storage and other applications. People are adopting new technology to achieve their required goals [1]. Cloud computing allows people to get a huge amount of data at high speed and large memory storage. Cloud data center consists of physical and virtual infrastructure resources which include servers, virtual machines (VMs), network infrastructure, and different resources [2]. Data centers (DC) are normally used to control various activities such as VM creation and destruction, routing of the user request, network management, resource utilization, and load balancing technique. Cloud computing architecture comprises of two main parts which are front end and back end where different components in term of storage, runtime, service and security work in back-end application and service work in front end [3], [4]. Cloud computing architecture consists of four layers. All layers are important due to their different operation and connectivity with each other. Different layers play important role for cloud computing. There are four types of cloud computing which are used in different field of life with specific rule and respective. Cloud computing is a general term for anything that involves in delivering hosted services over the internet. Cloud providers are

competing with each other and they constantly expand their services in order to differentiate themselves [5], [6]. Figure 1 present the structure of cloud computing. Cloud computing is named as such because the information being accessed is found remotely in the cloud or a virtual space. Cloud computing has succeeded in bringing change in different field of life. Main characteristic of cloud computing are availability, scalability, cloud security, cloud automation and virtualization [7]. Approval rating of cloud computing as an emerging technology has been enhanced significantly and these days, there are many cloud storage and computing providers who offer their services regarding IaaS, PaaS, and SaaS. Despite these considerable benefits there are serious concerns and challenges about this new technology [8]. Which are mention in Table 1 and Figure 2. Table 1 present all those challenges which are facing by cloud computing but one of the main issues is security in cloud computing. In this paper we cover all those security issues and their improvement technique for cloud computing.

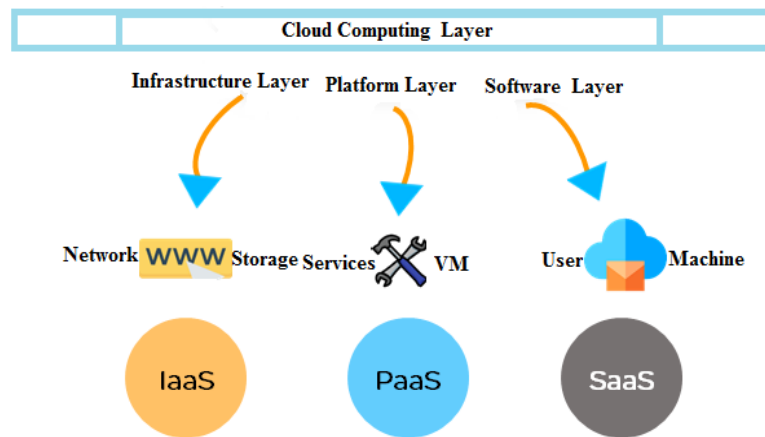


Figure 1. Structure of cloud computing

Table 1. Cloud computing challenges

Cloud computing	Challenges
Reliability	Possibility of failure in stand period of time
Interoperability	Lack of standards for service portability between cloud providers
Energy saving	Defining a standard metric for effective power usage and an efficient standard of infrastructure usage
Resiliency	The ability of the system to provide users with standard level of services while
Resource monitoring	Lack of accurate monitoring mechanism using sensors to collect the data from CPU load, memory
Load balancing	Lack of standard way of load monitoring and load management for different cloud applications
Security	Need improvement in security at different level of cloud computing [9]

## 2. INTERNET OF THINGS

Internet of thing (IoT) consists of self-configuration node they are connected with dynamic and with global network infrastructure. It comprises of small thing with limited storage and processing system. IoT refers a broad vision. Thing such ways that every day object is place environment are interconnected with each other with the help of internet [10]. As we know that IoT is important source of big data. Smart city is the main scores of data like industry, agriculture, traffic, transport, medical, public department and social, media. According to the process of data achievement and transmission in IoT the network architecture are divided in to three and five layers which are sensing layer, network layer and application layer [11]. Main element required for building IoT some of the main elements used for building IoT are, unique identification for each smart device, sensing devices, communication, data storage, analytics and visualization. Sensing devices each device contains sensing elements which used for different parameter like, sound level, motions, amount air, humidity and many more purpose [12]. In sensor network large number of nodes are installed for the requirement of interest. These smart sensor nodes are developed with the help of micro electro mechanical system and used for required purpose. Unique identification for each smart device IoT consists of unique identification number or label which are used to connection or used for uniqueness Ipv4 and ipv6 and other protocols are used for communication in IoT. Communication sense device sent data in to data base after collection of them through different communication mechanism, like near field communication (NFC), Wi-Fi, ultra-wide band (UWB), Z-wave, 3G, 4G, LTE-A data storage and analytics. IoT store large numbers of data for different environment and these data need to analysis then after they forward to data base. For analysis

purpose different algorithm and technique are used [13], [14]. Figure 2 presents the IoT structure along with communication devices.

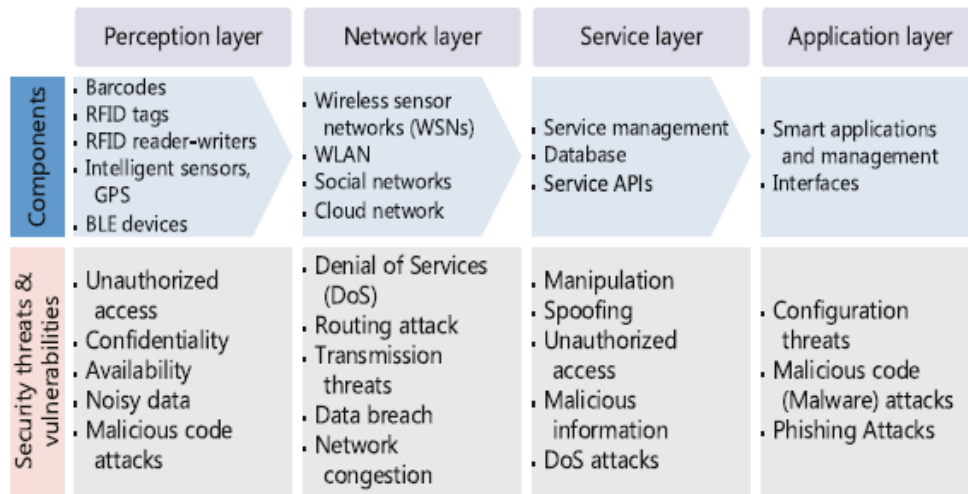


Figure 2. Structure of IoT [15]

Cloud computing and IoT are two different technologies with different architecture and characteristics both are important part in our life. Cloud computing is new technology that has significantly changed over the last decade. The deliveries of virtualized IT resource over the internet are performed with the help of it. These services are delivered with the rule of pay and gain on demand with real time service [16]. IoT become the next generation of technology it allows billions of internet device are connected and communicate with each other with specific rule and regulation it improves the quality of our daily life. Due to the modern world requirement these two technologies are merging together and known as cloud IoT paradigm. Cloud computing get more attraction and effectiveness due to the Integration with IoT in real world with distributed manner [17]. Table 2 shows the difference of both technologies. Table 2 shows the main difference of both technologies according to these differences they are managing to work together with specific rules and communication devices.

Table 2. Difference of two technologies

Cloud	IoT	Cloud	IoT
Virtual method used	Thing are passive	Virtual process has large store	Thing are real and on demand
Internet service delay	Limited storage capacity	Big data need to manage	Internet used for access coverage
Everyone can use resources	Big data store		Limited computation [18]

### 3. INTEGRATION RULE OF CLOUD COMPUTING AND INTERNET OF THING

After the study of literature, the integration of cloud computing with IoT consists of three steps which are minimal integration, partial integration and full integration. In minimal integration strategy this layer provided different layer that produce connection with cloud computing and IoT. It allows basic service like web, sensing storage and share these can be achieved with the help of these layers [19]. Partial integration in this integration not only middleware layer or platform layer are developed it provide smart object service provider. Its main role is to provide connection smart device connected with cloud computing and control them by multi-tenant approach. This layer provides virtualization for smart device [20]. Figure 3 present the integration of cloud computing and IoT [21].

The final stage of level integration is known as full integration strategy. This process merges new service models that contain or conversational all cloud computing layer. Simple we can say all layer are working collectively in this section [22]. Different heterogeneous network and framework and system with different patterns of communication like system to system, human to system and system to human. Cloud IoT is new birth of technology which service with different application that can impact in different field of life [23].

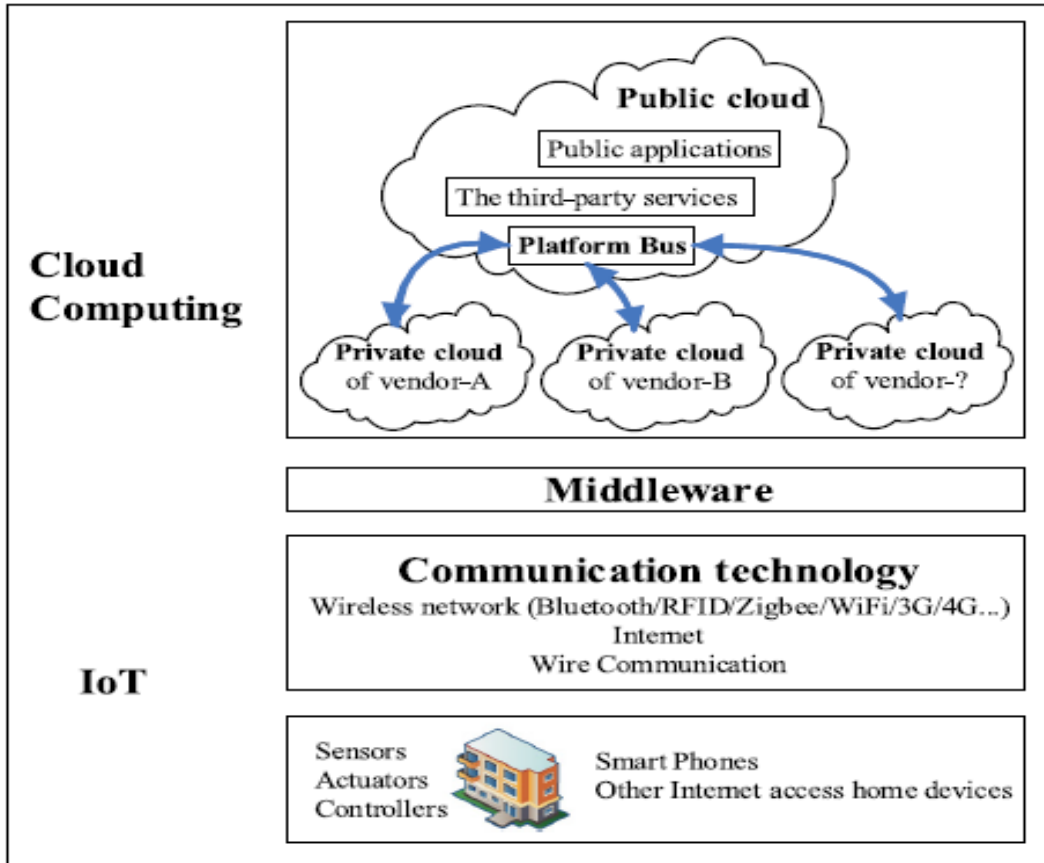


Figure 3. Integration of cloud computing and IoT

**4. SECURITY ISSUES IN INTERNET OF THINGS AND CC**

There is no doubt that the convenience and low cost of cloud computing services have changed our daily lives; however, the security issues associated with cloud computing make us vulnerable to cybercrimes that happen every day. The occurrence of the IoT has also dramatically altered the appearance of cyber threat. Security threats and vulnerabilities of IoT, industrial challenges, main reasons of cyber-attacks, cyber security requirement and some cyber security measures [24]. Some of the main security threats of both technologies are mention below. Table 3 present the security issue in cloud computing.

Table 3. Some of the famous attacks on cloud computing

Attacker name	Attacker incidents	Consequences	Category
VM rollback attack		Launch brute force attack Damage cloud infrastructure	Cloud infrastructure, access
Denial of service	Http-based DDoS Xml-based DDoS REST based-DDoS Shrew attack (light traffic) DoS	Leakage of sensitive information Service/hardware unavailability Wrapping a malicious code in Xml signature to gain unauthorized access to information	Network, cloud infrastructure
Theft-of service		Cloud service usage without billing Cloud resource stealing with less/no cost	Cloud infrastructure
Cross VM side channels	Energy consumption side channels	User data/information leakage cloud	Cloud infrastructure
Botnets	Stepping stone attack	Unauthorized access to cloud resources Make cloud system work abnormally Stealing sensitive information	Network, cloud infrastructure, access
Phishing		Unauthorized access to personal information Installing a malicious code into user computer	Cloud infrastructure, network, access
Cloud malware injection		Credential information leakage User data leakage Cloud machine abnormal behavior	Cloud infrastructure [25]

Malware attacker on VM: VM is one the main element of cloud computing as we know that virtualization is important section of cloud computing. When user sent data or request data from VM there will be unwanted VM based various or toolkit are used these kind of virus clock the information they sent user to VM or servers. Malwares or virus store the information such as registry, system log and security programs details. The attacker then used this information to their required goals [26]. Break of isolation: VM work as single or group or monitor each other it may affect by the attacker. Remote management vulnerabilities: commercial hypervisors normally have the control of management consoles and administrators to manage VM Xen for new faculties they may be affect by the attacker with the help of structured query language (SQL) injection [27]. Denial of service (DoS) vulnerabilities: in virtualization environment resource such as CPU, memory, networks are shared these resources are shared with user. It possible during execution it chance that DoS attack during the system when user request for resource then it shows that no resourced available [28]. Revert to snapshots problem: snapshot is a mechanism is process in which a administrator make snapshot for machine in certain point and to revert to the some security and if need some information the snapshot used some time its disabled due to attacker and make issue for the system [29]. Destruction: when the data is no more required then it needs destruction the question arises that the data destroy or not because the physical characteristic of storage medium the data may be restored [30]. Archival: archival of data deals with the storage of data in cloud storage medium where that is store offline or online and can be access able within cloud or connected network. Sometime data storage occurs where it may be offline or not connected with the network for some time or period of time then the data primary and security issue or threat will be there [31]. Transfer: confidentiality and integrity of data are one of the main elements and both must apply any form of data transfer process. This process not applies between the enterprise or cloud storage but also apply between different storage [32]. Storage: in cloud computing data storage divided into two main environment IaaS environment and SaaS environment and different storage setup are used. For data security, reliability, accuracy, backup, and data management system need more reliable system [33].

## 5. INTERNET OF THINGS SECURITY ISSUES

The domains of security attacks on different hybrid device are increasing day by day. The following Figure 4 show summaries of attackers. Now a day's IoT has the most adoption in term of new device connection through with the help of internet. Every day these smart devices become under target of attacker they try different method to get their required goals. As we know that different layer is there in IoT and attacker target these layer [34].

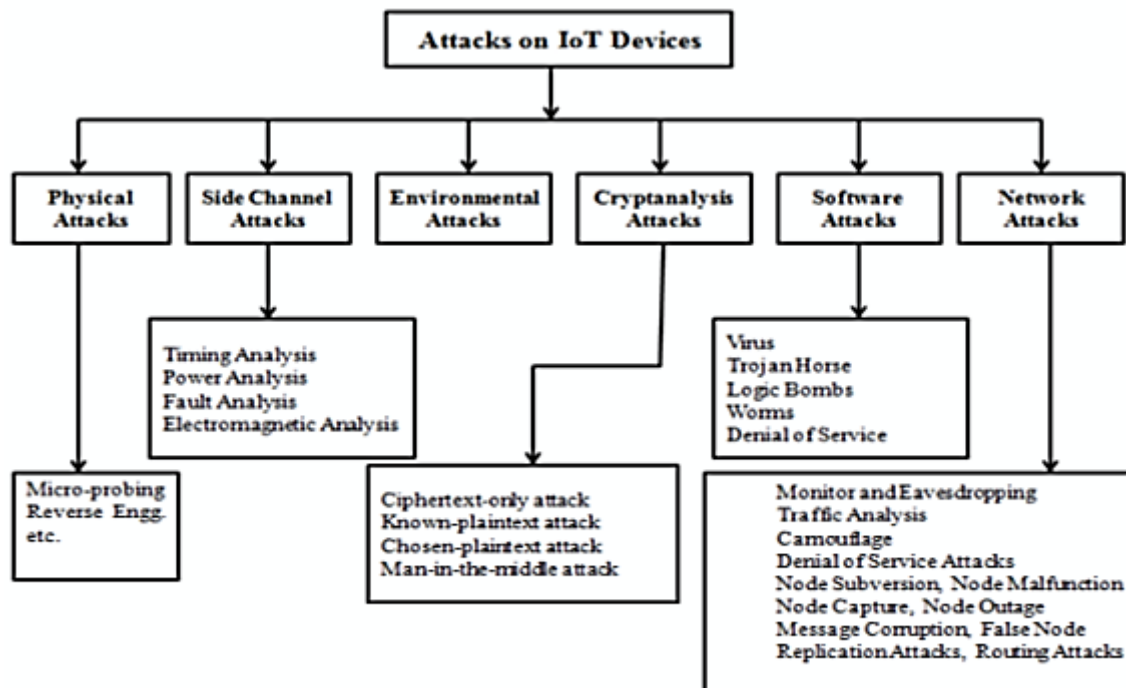


Figure 4. Different attack on IoT devices [35]

Physical attacker: in IoT physical attacker means all those attacks which are tamper on hardware components and try miss use or de-packaging of chip, layout or damaged physical device. Or may miss user the physical components [36]. Threats for application layer: the personalized services based on the needs of the users are included in the application layer; e.g. the interface that user can control devices in IoT. Threats in this layer mainly target these services as mentioned areas [37]. Sniffer/Loggers are those programs or hacker code which user used or attacker can used to hack the system password. The attacker used this kind of code used for network traffic. The main goals of this sniffer is to steal password file, like (FTP, e-mail file, email text and many other protocols [38]. Injection: when attacker tries to attack on application servers with help of some code that is known as injection. This kind of attack are simple and simple code are used they affect the data, loss data or corruption and lack of accountability [39]. Social engineering this of attacks are performed with the help of social media like chat, email searching and may more. This kind of attacker can affect data and system like hardware and software [38]. Distributed DoS (DDoS) it work same as the DoS attack but in this same more attacker attack the same target and multiple point and search for same goal [40]. Sessions hijacking this kind of attack are performed in authentication session of management. They use personal identities or try to hacker the system by getting the person information. These kinds of attack are simple and common and attackers can try at any place and any time without problems [41]. Threat of support layer: target of threats in support layer is mainly data storage technologies. These threats are discussed are as: tampering with data this kind of attack is performed by third party the change or temped data for their personal benefit or organization benefit. Data modification took place by any attacker group or their benefit that is known as tampering with data [42]. DoS attack as pervious expiation this kind of attacker are also performed in this layer also. Unauthorized access different attackers are trying to get data from IoT by try unauthorized access. Threats of perception layer: sensor and intelligence embedded technologies including RFID readers, sensors or GPS are under threat because of various security flaws. Main threats are discussed area as: spoofing this kind of attack are performed with the help of broadcast message and these message are sent to sensor network and it make surety like as it is actual message and the attacker get access the sensor network and making vulnerable to the network [43]. Radios jamming this kind of attack are performed with communication system like communication channel, communication method the attacker work as DoS attacker do and this kind of attract affect the communication channel [44]. Device tamping in this kind of attack the user capture the sensor node or replace the node with other physical device and get total control on the sensor network. Path based DoS attack (PDoS) in this type of attack the overpower and path or communication channel. This type of attack are performed end to end communication [45]. Centre node destroy in some situation the entire sensor network depends on one single node if the centre node destroy the full sensor network fall and the attacker try to damage the centre node and make the network fall [46]. Eavesdropping some time the attacker try to sniffs the RFID tags and read the basic information and change password or confidential information and the attacker try to get important information [47]. Threats of network layer: network layer which is known as the next-generation network are exposed to many kinds of threats. Related threats that come from this layer are listed are as: selective forwarding in this kind attack some node does not forward message and sent some selectivity drop the attracter hake them and they not reply as normal message and these are called selective forwarding. There are different types of selective forwarding attackers and use DoS for forward message traffic system [48]. Sybil attack it is clarified as malicious and taking multiple identities for attack one or more place at one or the attacker used multiple identities to the node or different nodes and reduce the device capacity or make fault tolerant scheme [49]. Wormhole this form of attack make changes in data bit form and change the position of bit of data and it make low latency in the network or device. Man-in-middle attack these kinds of attacker make eavesdropping and the unauthorized parties check and control all the private message or communication. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information [50]. Hello-flood attack in this kind of attack the single malicious device sent single message and it replicate the message and make multiple messages in this form it attacks on traffic Physical attackers: these types of attacks tamper with the hardware components and are relatively harder to perform because it requires expensive material. Some examples are de-packaging of chip, layout reconstruction, micro-probing, and particle beam techniques [51].

## 6. IMPROVEMENT IN SECURITY ISSUES FOR CC AND INTERNET OF THINGS

In this section we present those algorithm and technique for improvement of these section improve the cloud computing and IoT are mention. Table 4 present those algorithms which are used for different purpose in security section for improvement of these techniques improve different section of cloud computing and IoT. Table 5 present the different layer of CC and IoT. For protection of these different techniques are used.

Table 4. Cryptographic algorithms

Type	Algorithm	Purpose
Hashing	SHA-1/SHA-256	Integrity
Asymmetric key agreement	Diffie-hellman (DH)	Key agreement
Symmetric encryption	Advanced encryption standard (AES)	Confidentiality
Asymmetric encryption	Rivestshamir adelman (RSA)/Elliptic curve cryptography (ECC)	Digital signatures, key transport
	AES	Confidentiality
	RSA/ECC	Digital signatures, key transport
	Diffie-hellman (DH)	Key agreement
	SHA-1/SHA-256	Integrity [38]

Table 5. Layer attacks in CC and IoT

Layers	Attacks	Defenses
Physical	Jamming radio interference	Channel surfing, spatial retreat,
	Tampering	Priority messages
MAC	Radio interference delayed disclosure of keys tampering	Radio interference delayed disclosure of keys
Network	tamper-proofing, hiding collision, exhaustion, unfairness	Tampering tamper-proofing, hiding
	Sinkhole	Authorization, monitoring,
	Worm/black hole	redundancy, encryption, egress filtering,
Transport	Misdirection	authorization, monitor
	De-synchronization	Client puzzles
Application	Flooding	Authentication
	Flooding, overwhelm, reprogram	Rate-limiting, authentication [52]

Table 5 present different layers in CC and IoT where different attacker attached using different technique which is mention in Table 5 and for security of these attacks different research improved different section taking different algorithm. Table 6 present cloud computing layer and their descriptions. Table 6 present the different cloud layer description and the standard rule safe and protect from different attackers. We improve different section using and improving these standard technique or algorithms. Table 7 present the different attacks which are performed on IoT devices for improvement in these IoT devices different research improving algorithm and framework of the devices.

Table 6. Cloud computing layer description

Category	Description
Security standards	Describes the standards required to take precaution measures in cloud computing in order to prevent attacks. It governs the policies of cloud computing for security without compromising reliability and performance.
Network	Involves network attacks such as connection availability, DoS, DDoS, flooding attack, and internet protocol vulnerabilities.
Access control	Covers authentication and access control. It captures issues that affect privacy of user information and data storage.
Cloud infrastructure	Covers attacks that are specific to the cloud infrastructure (IaaS, PaaS and SaaS) such tampered binaries and privileged insiders.
Data	Covers data related security issues including data migration, integrity, confidentiality, and data warehousing [53]

Table 7. Security issues in IoT

IoT	Attack section need improvement	IoT	Attack section need improvement
Traffic analysis	Traffic analysis countermeasure	Countermeasure against jamming	Regulated transmitted power
Countermeasure	Countermeasure against eavesdropping	Layer	Physical layer identification
Countermeasure	Countermeasure against sybil attacks	Context oriented	Traffic analysis, tempering attacks: tag modification
Data oriented	Eavesdropping	WSN attacks	Need improvement
DoS	Need improvement	RFID attacks injection [13], [54]	Need improvement

## 7. CONCLUSION

Cloud computing provide different type of network where they location different location and produce all information to the end user. The cloud computing provides different services to their clients called front end and the cloud itself refer as back end that provides such services to the clients. One of the main challenges related to cloud computing called data security of multiple clients. One of the critical challenges facing interacting with IoT devices is addressing billions of devices (things) around the world, including: computers,



tablets, smart phones, wearable devices, sensors and embedded computers, and the main issues is the security of these devices. This paper provided review of different security aspects of cloud computing and IoTs at different layers and section in the network. In this review paper we have discuss the security aspect of cloud and IoT as well as we make the problem formulation of security and future research direction.

## REFERENCES




- [1] W. Hassan, T.-S. Chou, X. Li, P. A-Kubi, and T. Omar, "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 8, no. 3, p. 162, Dec. 2019, doi: 10.11591/ijict.v8i3.pp162-183.
- [2] W. Hassan, T.-S. Chou, O. Tamer, J. Pickard, P. A.-Kubi, and L. Pagliari, "Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 9, no. 2, p. 117, Aug. 2020, doi: 10.11591/ijict.v9i2.pp117-139.
- [3] G. Giannopoulou *et al.*, "DOL-BIP-critical: a tool chain for rigorous design and implementation of mixed-criticality multi-core systems," *Design Automation for Embedded Systems*, vol. 22, no. 1–2, pp. 141–181, Jun. 2018, doi: 10.1007/s10617-018-9206-3.
- [4] A. Ullah, C. B. Şahin, O. B. Dinler, M. H. Khan, and H. Aznaoui, "Heart disease prediction using various machines learning approach," *Journal of Cardiovascular Disease Research*, vol. 12, no. 3, pp. 379–391, 2021.
- [5] H. Aznaoui, A. Ullah, S. Raghay, L. Aziz, and M. H. Khan, "New efficient GAF routing protocol using an optimized weighted sum model in WSN," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, p. 396, Apr. 2021, doi: 10.11591/ijeecs.v22i1.pp396-406.
- [6] A. Ullah, N. M. Nawati, A. Arifianto, I. Ahmed, M. Aamir, and S. N. Khan, "Real-time wheat classification system for selective herbicides using broad wheat estimation in deep neural network," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 9, no. 1, p. 153, Jan. 2019, doi: 10.18517/ijaseit.9.1.5031.
- [7] S. N. Khan, N. M. Nawati, M. Imrona, A. Shahzad, A. Ullah, and A.-Rahman, "Opinion mining summarization and automation process: a survey," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 5, p. 1836, Oct. 2018, doi: 10.18517/ijaseit.8.5.5002.
- [8] S. N. Khan *et al.*, "Comparative analysis for heart disease prediction," *JOIV: International Journal on Informatics Visualization*, vol. 1, no. 4–2, p. 227, Nov. 2017, doi: 10.30630/joiv.1.4-2.66.
- [9] K. Xing, S. S. R. Srinivasan, M. J. Rivera, J. Li, and X. Cheng, "Attacks and countermeasures in sensor networks: a survey," in *Network Security*, Springer US, 2010, pp. 251–272, doi: 10.1007/978-0-387-73821-5\_11.
- [10] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A Survey on Supply chain security: application areas, security threats, and solution architectures," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6222–6246, Apr. 2021, doi: 10.1109/jiot.2020.3025775.
- [11] A. Llaría, J. D. Santos, G. Terrasson, Z. Boussaada, C. Merlo, and O. Curea, "Intelligent buildings in smart grids: a survey on security and privacy issues related to energy management," *Energies*, vol. 14, no. 9, p. 2733, May 2021, doi: 10.3390/en14092733.
- [12] H. Adkins, B. Beyer, P. Blankinship, P. Lewandowski, A. Oprea, and A. Stubblefield, "Building secure & reliable systems: best practices for designing, implementing and maintaining systems," *Gravenstein Highway North*, Sebastopol, CA, Amerika Serikat: O'Reilly Media, 2020.
- [13] D. Sebai and A. U. Shah, "Semantic-oriented learning-based image compression by only-train-once quantized autoencoders," *Signal, Image and Video Processing*, Apr. 2022, pp. 1–9, doi: 10.1007/s11760-022-02231-1.
- [14] N. Volianska, O. Sadovoi, and R. Voliansky, "Transformation of the generalized chaotic system into the discrete-time complex domain," *Jurnal Informatika*, vol. 15, no. 1, pp. 56–67, Jan. 2021, doi: 10.26555/jifo.v15i1.a20222.
- [15] A. N. Rao, R. Naik, and N. Devi, "On maximizing the coverage and network lifetime in wireless sensor networks through multi-objective metaheuristics," *Journal of The Institution of Engineers (India): Series B*, vol. 102, no. 1, pp. 111–122, Nov. 2020, doi: 10.1007/s40031-020-00516-y.
- [16] A. Ullah, N. M. Nawati, and S. Ouhamme, "Recent advancement in VM task allocation system for cloud computing: review from 2015 to 2021," *Artificial Intelligence Review*, vol. 55, no. 3, pp. 2529–2573, Sep. 2021, doi: 10.1007/s10462-021-10071-7.
- [17] S. Ouhamme, Y. Hadi, and A. Ullah, "An efficient forecasting approach for resource utilization in cloud data center using CNN-LSTM model," *Neural Computing and Applications*, vol. 33, no. 16, pp. 10043–10055, Mar. 2021, doi: 10.1007/s00521-021-05770-9.
- [18] H. Shah, M. Shah, S. Tanwar, and N. Kumar, "Blockchain for COVID-19: a comprehensive review," *Personal and Ubiquitous Computing*, Aug. 2021, pp. 1–28, doi: 10.1007/s00779-021-01610-8.
- [19] M. K. Ahsan, "Increasing the predictive potential of machine learning models for enhancing cybersecurity," *North Dakota State University*, 2020. [Online]. Available: <https://library.ndsu.edu/ir/handle/10365/32291>.
- [20] K. N. Isnaini and S. A. Solikhatin, "Information security analysis on physical security in university x using maturity model," *Jurnal Informatika*, vol. 14, no. 2, p. 76–84, May 2020, doi: 10.26555/jifo.v14i2.a14434.
- [21] O. A. Simon, U. I. Bature, K. I. Jahun, and N. M. Tahir, "Electronic doorbell system using keypad and GSM," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 9, no. 3, p. 212, Dec. 2020, doi: 10.11591/ijict.v9i3.pp212-220.
- [22] S. Ouhamme, Y. Hadi, and A. Arifullah, "A hybrid grey wolf optimizer and artificial bee colony algorithm used for improvement in resource allocation system for cloud technology," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 16, no. 14, pp. 4–17, Nov. 2020, doi: 10.3991/ijoe.v16i14.16623.
- [23] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, Sep. 2020, doi: 10.1016/j.iot.2020.100218.
- [24] N. Redini, "Analyzing and securing firmware for IoT devices," Ph.D. dissertation, Dept. Comput. Sci., Univ. of California Santa Barbara, Santa Barbara, CA, United States 2020. [Online]. Available: <https://escholarship.org/uc/item/4zr7639m>.
- [25] T. F. Prasetyo, R. Rohmat, and D. Zalilluddin, "Design and build disaster emergency response systems using firebase cloud messaging based on android and SMS gateway," *Jurnal Informatika*, vol. 13, no. 1, pp. 16–24, Jan. 2019, doi: 10.26555/jifo.v13i1.a11664.
- [26] I. T. Mulyawan and A. Prahara, "Motorcycles detection using haar-like features and support vector machine on CCTV camera image," *Jurnal Informatika*, vol. 13, no. 2, pp. 32–39, Jul. 2019, doi: 10.26555/jifo.v13i2.a13194.
- [27] V. Passricha, A. Chopra, P. Sharma, and S. Singhal, "A secure deduplication scheme for encrypted data," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 8, no. 2, pp. 77–86, Aug. 2019, doi: 10.11591/ijict.v8i2.pp77-86.






- [28] J. Ferdous, Md. F. N. Khan, K. M. Rezaul, M. A. Tamal, Md. A. Aziz, and P. Miah, "A hybrid framework for security in cloud computing based on different algorithms," *International Journal of Network Security*, vol. 22, no. 4, pp. 638–644, May 2020.
- [29] D. D. Fagbemi, D. M. Wheeler, and J. Wheeler, "The IoT architect's guide to attainable security and privacy," 1<sup>st</sup> Edition. Auerbach Publications-CRC Press, 2019. [Online]. Available: <https://www.routledge.com/The-IoT-Architects-Guide-to-Attainable-Security-and-Privacy/Fagbemi-Wheeler-Wheeler/p/book/9780815368168>.
- [30] R. Sulaiman, "Combination and comparison of AES and RC4 cryptography in least significant bit (LSB) method in digital image to improve message security," *Jurnal Informatika*, vol. 12, no. 2, pp. 45–52, Jul. 2018, doi: 10.26555/jifo.v12i2.a8667.
- [31] I. Riadi, R. Umar, and W. Sukarno, "Vulnerability of injection attacks against the application security of framework based websites open web access security project (OWASP)," *Jurnal Informatika*, vol. 12, no. 2, pp. 53–57, Jul. 2018, doi: 10.26555/jifo.v12i2.a8292.
- [32] S. Sharma, "A state of art on energy efficient multipath routing in wireless sensor networks," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 7, no. 3, pp. 111–116, Dec. 2018, doi: 10.11591/ijict.v7i3.pp111-116.
- [33] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, Nov. 2018, doi: 10.3390/s18113907.
- [34] F. Firouzi, B. Farahani, M. Ibrahim, and K. Chakrabarty, "Keynote paper: from EDA to IoT eHealth: promises, challenges, and solutions," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 12, pp. 2965–2978, Dec. 2018, doi: 10.1109/tcad.2018.2801227.
- [35] P. Srivastava and A. Mostafavi, "Challenges and opportunities of crowdsourcing and participatory planning in developing infrastructure systems of smart cities," *Infrastructures*, vol. 3, no. 4, p. 51, Nov. 2018, doi: 10.3390/infrastructures3040051.
- [36] N. Kurniasih, "Internet addiction, lifestyle or mental disorder? a phenomenological study on social media addiction in Indonesia," *KnE Social Sciences*, vol. 2, no. 4, pp. 135–144, Jun. 2017, doi: 10.18502/kss.v2i4.879.
- [37] S. Ravichandran, "Cloud connected smart gas cylinder platform senses LPG gas leakage using IOT application," *International Journal of MC Square Scientific Research*, vol. 9, no. 1, pp. 324–330, Apr. 2017, doi: 10.20894/ijmsr.117.009.001.038.
- [38] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.
- [39] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33–50, Jun. 2017, doi: 10.1016/j.adhoc.2017.03.006.
- [40] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3655–3682, Apr. 2016, doi: 10.1007/s00521-016-2317-5.
- [41] J. Shahid, S. Saleem, and M. N. Qureshi, "DOS attacks on WSN and their classifications with countermeasures-a survey," *NUST Journal of Engineering Sciences*, vol. 9, no. 2, pp. 50–59, Dec. 2016, doi: 10.24949/njes.v9i2.281.
- [42] P. Meharia, "Secure trust establishment in an internet of things framework," Ph.D Thesis. University of Cincinnati, 2016.
- [43] T. Alam, "5G-enabled tactile internet for smart cities: vision, recent developments, and challenges," *Jurnal Informatika*, vol. 13, no. 2, pp. 1–10, Jul. 2019, doi: 10.26555/jifo.v13i2.a13426.
- [44] K. A. Anderson, "The frugal CISO: using innovation and smart approaches to maximize your security posture," 1<sup>st</sup> edition. Boca Raton, FL: Auerbach Publications-CRC Press, 2014.
- [45] M. P. Singh and P. Kumar, "An efficient forward error correction scheme for wireless sensor network," *Procedia Technology*, vol. 4, pp. 737–742, 2012, doi: 10.1016/j.protcy.2012.05.120.
- [46] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008, doi: 10.1109/comst.2008.4625802.
- [47] M. C. Huebscher and J. A. McCann, "A survey of autonomic computing—degrees, models, and applications," *ACM Computing Surveys*, vol. 40, no. 3, pp. 1–28, Aug. 2008, doi: 10.1145/1380584.1380585.
- [48] H. W. Kim and S. Lee, "Design and implementation of a private and public key crypto processor and its application to a security system," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 214–224, Feb. 2004, doi: 10.1109/tce.2004.1277865.
- [49] S. Umar, S. Baseer, and Arifullah, "Perception of cloud computing in universities of Peshawar, Pakistan," *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, Aug. 2016, pp. 87–91, doi: 10.1109/intech.2016.7845046.
- [50] Arifullah, S. Baseer, and S. Umar, "Role of cooperation in energy minimization in visual sensor network," *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, pp. 447–452, Aug. 2016, doi: 10.1109/intech.2016.7845026.
- [51] J. Grover and S. Sharma, "Security issues in wireless sensor network—a review," *2016 5<sup>th</sup> International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 397–404, Sep. 2016, doi: 10.1109/icrito.2016.7784988.
- [52] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in VANET," *International Journal of Computer Applications*, vol. 66, no. 22, pp. 45–49, Mar. 2013.
- [53] M. Meghdadi, S. Ozdemir, and I. Güler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *IETE technical review*, vol. 28, no. 2, pp. 89–102, 2011, doi: 10.4103/0256-4602.78089.
- [54] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the internet of things: a comprehensive investigation," *Computer Networks*, vol. 160, pp. 165–191, Sep. 2019, doi: 10.1016/j.comnet.2019.05.014.

## BIOGRAPHIES OF AUTHORS






**Arif Ullah**    completed my Ph.D. in cloud computing with 2 years of experience in teaching and research. His area of expertise in cloud computing, IoT. Areas of interest include software defined networking (SDN), load balancing, switches migration, WSN, E-learning, AI, WSN, and security. He can be contacted at email: [arifullah@riphahfsd.edu.pk](mailto:arifullah@riphahfsd.edu.pk).






**Imane Laassar**    working as Research Assistant Department of Mathematics, Université Ibn Tofail at Morocco. Research interests are artificial intelligence, computer security and reliability, computing in mathematics, natural science, and engineering and medicine. She can be contacted at email: [imane.laassar@gmail.com](mailto:imane.laassar@gmail.com).






**Canan Batur Şahin**    receive her diploma and Ph.D degrees in Computer Engineering from Yildiz Technical University. Her research interests include software engineering, artificial intelligence, and optimization. She can be contacted at email: [canan.batur@ozal.edu.tr](mailto:canan.batur@ozal.edu.tr).



**Ozlem Batur Dinle**    is work in Department of Computer Engineering, Siirt University, Turkey. Her research interests include artificial intelligent, machine learning, and deep learning, and software engineering. She can be contacted at email: [canan.batur@ozal.edu.tr](mailto:canan.batur@ozal.edu.tr).



**Hanane Aznaoui**    working as Research Assistant at Laboratory of Applied Mathematics and Computer Science, Department of Computer Science. Research interests are routing protocols, routing, wireless sensor network, computer, networking, network, communication, and network simulation. She can be contacted at email: [h.aznaoui@gmail.com](mailto:h.aznaoui@gmail.com).