Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.019837
Article

Cloud-IoT Integration: Cloud Service Framework for M2M Communication

Saadia Malik[1], Nadia Tabassum[2], Muhammad Saleem[3], Tahir Alyas[4], Muhammad Hamid[5,*] and Umer Farooq[4]

[1]Department of Information Systems, Faculty of Computing and Information Technology - Rabigh, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Computer Science, Virtual University of Pakistan, Lahore, 54000, Pakistan
[3]Department of Industrial Engineering, Faculty of Engineering, Rabigh, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[4]Department of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan
[5]Department of Statistics and Computer Science, University of Veterinary and Animal Sciences, Lahore, 54000, Pakistan
*Corresponding Author: Muhammad Hamid. Email: muhammad.hamid@uvas.edu.pk
Received: 27 April 2021; Accepted: 04 June 2021

Abstract: With the ongoing revolution in the Internet of Things (IoT) and cloud computing has made the potential of every stack holder that is connected through the Internet, to exchange and transfer data. Various users perceive this connection and interaction with devices as very helpful and serviceable in their daily life. However, an improperly configured network system is a soft target to security threats, therefore there is a dire need for a security embedded framework for IoT and cloud communication models is the latest research area. In this paper, different IoT and cloud computing frameworks are discussed in detail and describes the importance of the daily life of people. The main focus is to design the Cloud-IoT integration that is used to implement IoT and Cloud Framework for M2M communication, also building a relationship between different devices to connect through a cloud and also find different security methods to secure those devices. Extensive papers finding and results showed different ways they have been introduced to manipulate M2M in the digital field of health care and the virtual world. While focusing on the methodology used in M2M it is also imperative to concentrate on security levels from different inside and outside attacks on IoT and cloud ecosystem. There is a need to create a strong and secure connection between all of our IoT devices with a cloud so that there should be a fixed and safe connection between cloud environments concerning M2M connection between all wired and wireless devices. Meanwhile in contemplation of security mode also conducive to maintain M2M connection between IoT devices and Cloud and in which areas these methodologies have been implemented.

Keywords: Machine communication; machine performance; device vulnerability; internet of things; virtualization security

1 Introduction

The model of the Internet of Things (IoT) is grounded on self-configuring nodes that are connected in a wide foundation network. Practically IoT is distinguished by small things, globally dispensed attached with limited storage along with limited processing volume. On the other side, the cloud with its immense storage and processing power, virtually played an important role to assist the IoT Ecosystem by providing significant application-specific services in various IoT application domains [1].

As the Internet of things (IoT) and cloud computing technologies are being considered as the imperative topics researched globally, so the Internet of things and cloud computing both are offering their imperative role in Information Technology and both technologies perform an emerging behavior in the future on the internet. Whereas Cloud computing has its different paradigms to acquire its services or platform for a specific environment. Additionally, their emerging trends have increased the value of the Information Technology platform. After discussing a precise background it is easy to understand the foundation of the Internet of Things and Cloud, therefore, In Fig. 1 shows the communication flow where the cloud is the main storage medium and various IoT devices data, sensors data, and applications records are connected and storing data with the centralized cloud via the Internet [2].

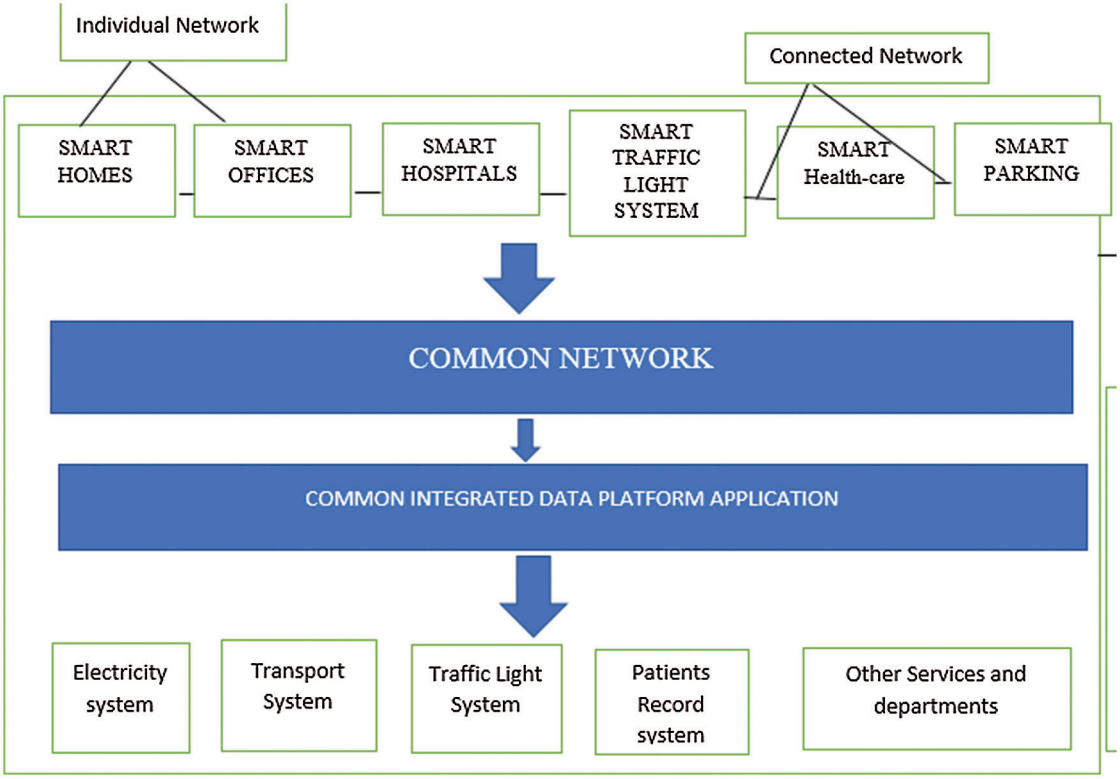

Figure 1: IoT services and applications

On the cloud side, many other devices have also been connected and exchanging information about data records of medical healthcare machines and other electrical appliances to make a strong connection. Currently, IoT consists of a various sensory collection of disparate, purpose-built networks devices. In Today's era, cars, for instance, have multiple systems or networks to control engine function, safety features, communications framework, and so on. Business and private structures additionally include several control systems for heating, venting, and air conditioning (HVAC); telephone utility; security; and

lighting. As IoT evolves, these networks, and numerous other sectors of daily life, related to added security, analytics, and management capabilities as shown in Fig. 1. This will enable IoT to turn into even more capable and powerful in what it can help individuals to accomplish [3].

The connectivity of billion IoT devices is the major challenge in the IoT world and current technologies and communication models should be adjusted to address the challenge of scalability. The reliability of the data center's resources/services is measured based on the following three security issues are the major issue of cloud IoT networks because the IoT network and its related nodes are connected to the Internet to exchange data and information. When an IoT device passes all the following various security concerns and attacks then we consider such IoT device secured [4].

Cloud computing is a hosted service provided over the internet. It provides high-performance computing of millions of instructions per second. In today's era, the concept of cloud computing has grown up from a developing advanced architecture to one of the fastest-growing IT segments. As the advantages of Cloud computing enhanced many service providers, provide cloud service in numerous models. Cloud computing consists of a combination of technologies that are used to achieve any task like multiprocessors, network-based distributed computing systems, and space to store, retrieve data. It handles multiple task requests from many users or clients concurrently. It reduces resources, installation, and maintenance costs and data can accesswhenever you need it. Organizations and companies that need to compute large transactions or computations daily need more hardware support, space, speed to perform their tasks, cloud computing facilitates them with a highly functional environment to perform computations [4].

IoT consists of interrelated devices such as sensors, smartphones, and wearables with the ability to transfer data over the network without any human-to-human or human-to-machine intervention. It is a component that is part of the centralized cloud and it stores the aggregated data of IoT devices.

A centralized controller is a core component of the proposed framework that is responsible for managing the execution of other components in the network. This controller tells its affiliated router what action is to perform on what device and which packet is to send towards what device or component. The centralized controller is directly connected to a router that has a routing table stored in it as shown in Fig. 2. That routing table contains information such as flow entries and their perspective rules, data entries, and its perspective rules.

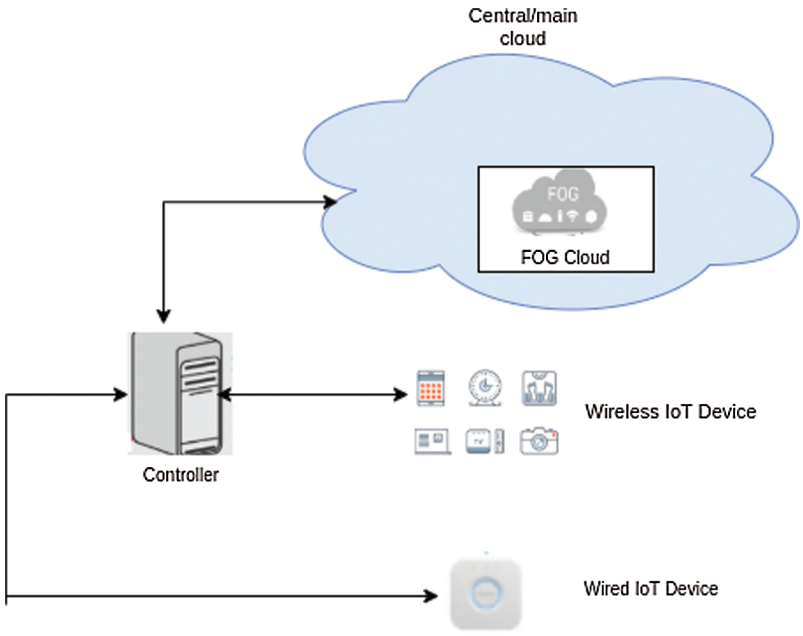

Figure 2: IoT-cloud integrated model

2 Related Work

Ghobaei-Arani et al. [5] proposed an IoT We-Care system for elderly people's health and their health can be monitored with the help of a wristband. It is a comfortable wristband that is ready to provide elderly living assistance and that can monitor and enroll patients along with their data. In case, any tragedy occurs this wristband is also capable of generating alarms and medical emergencies when victims are in a kind of trauma and not able to properly deliver information regarding themselves. So, in that case, a dedicated device is used and that is an IoT-based device and it provides virtual assistance to doctors to provide information regarding the identification of patients or patients along with medical information of every victim. This dedicated device is a wearable identity that has a unique identification number.

Hong et al. [6] proposed a system that works for infant health monitoring. This system keeps track of important parameters like body temperature, movement of that infant as well as pulse rate. This model is designed by keeping in mind mothers of 3rd world countries, when they are away from their newborns or out from home for the sake of work. This system is composed of a temperature sensor, pulse sensor, voice sensor, motion sensor, and these sensors give information to microcontrollers. This microcontroller is also attached with a power supply and a Wi-Fi module with the help of the internet send information to a database of phone or laptop or any device which is part of this system.

Mohanty et al. [7] work on making campus life smart with IoT help. They proposed the concept of "smart classrooms" where students can access their helping material anytime, anywhere. On the other side, lecturers can use smartphones and wearable devices to enhance their teaching skills as well as to engage students during lecture delivery. This smart classroom facilitates students and teachers with the help of sensors, controllers, and several physical objects. Naz et al. [8] proposed an IoT-based smart home system in which multiple systems are part of the main system. Subsystems are monitoring the critical parameters like electricity appliances control system, home security system, energy-saving system, monitoring along with alert, etc. A smart application is used by an authenticated user which has his login id along with a password to check the status of every IoT device. It is a hardware-based system in which the sleep and wake mode of different devices is being used to increase the energy efficiency of the system.

Neagu et al. [9] also proposed a smart home called an IoT Smart Home System (IoTSHS) which consist of remote control to a smart home with the help of mobile, microcontroller (Wi-Fi based), Infrared (IR) remote control along with PC/Laptop, temperature sensor (that will tell AC is required to be ON/OFF at this point of time), relays (that will act as ON/OFF switches and power distribution box. This type of model provides comfort to people who are not happy in using or cannot use mobile phone applications.

Neupane et al. [10] proposed a garbage collection management system that uses ultrasonic sonic sensors on garbage cans. This sensor tells about can level (if it is filled or not) and then it sends data to servers over an online application programming interface (API). This API stores different information like filled time, clean up time, and location, where can, is filled. This algorithm also gives suggestions on where another garbage can be installed. Priya et al. [11] also proposed a cost-effective and eco-friendly solid waste management system that provides a real-time interface. It also gives details of semi-empty bins of the city and tells what numbers of bins and vehicles should be used in the city.

Xuan et al. [12] proposed a system that helps to improve crop quality in agriculture with the use of IoT. This system uses drones and that consists of sensors, cameras, equipped modules. The proposed model of this paper consists of an RGB D sensor (depth-sensing sensor), Gas Sensor, GPS module and all these are giving information to Raspberry Pi Module which finds out about seed and pesticide sprayer. This microcontroller also saves information in the backend cloud for further use [13].

3 Proposed Methodology

We have proposed a structure for the secure integration of IoT (computing devices) with cloud systems. We have interconnected cloud and IoT devices with a centralized controller. To examine security controls that can be used to secure IoT system data and cloud data. Therefore, ubiquitous access to different types of information would be allowed through proposed centralized controllers which will help in terms of significant improvement in protecting data. Additionally, a sub-cloud layer is made part of a centralized cloud that is proficient enough to store aggregated data. Every node has assigned different keys to communicate with all nodes whose authenticity is checked by the controller.

Fig. 3 shows the sharable proposed architecture. In this framework, the IoT network (consisting of wired and wireless IoT nodes) and cloud systems are orchestrated by the main controller. This main controller is the main hub of the entire network because it has been set up to guarantee cybersecurity attack prevention that can otherwise create a halt in the network. The selection of operating with a single controller is due to the reason that a single controller has better performance to manage the traffic of a set of medium-size IoT networks along with cloud systems.

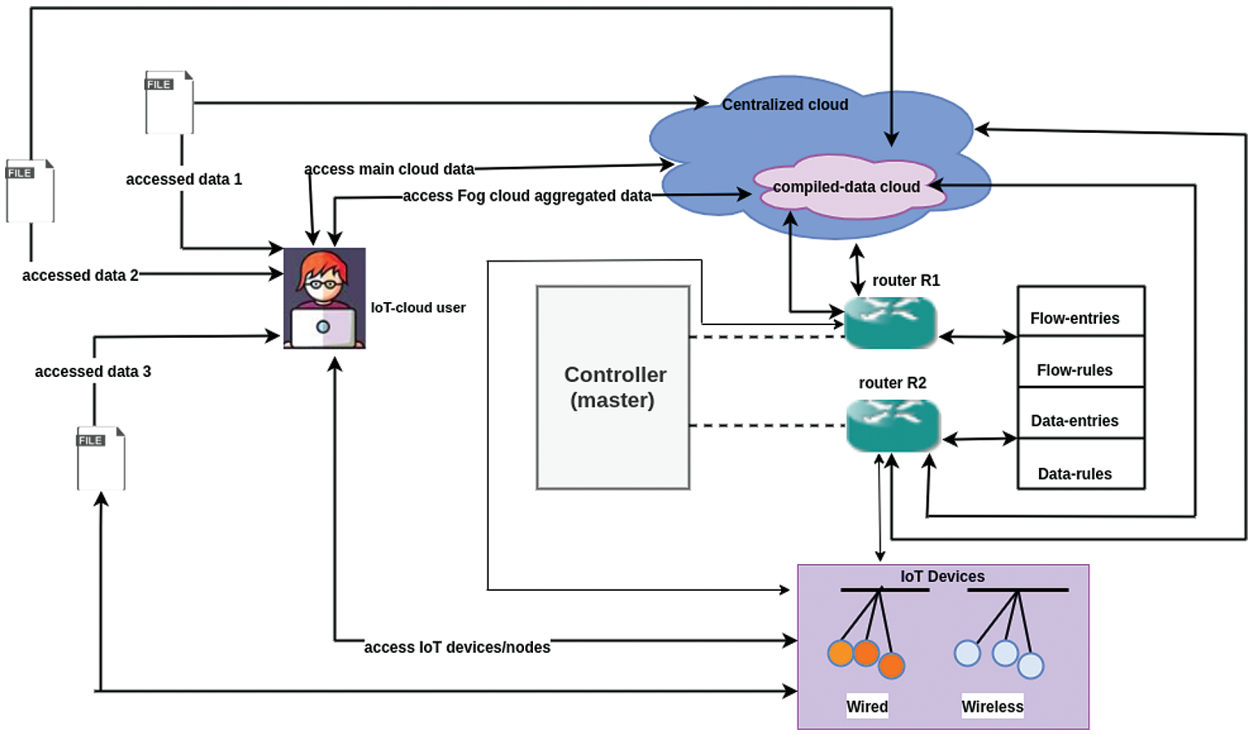

Figure 3: IoT-cloud secured model

The master controller is further connected to a router which is a core component in the proposed structure because it can flow traffic within the complete network as per instructions set by the controller. The router contains flow entries, flow rules, data entries, and data rules within its table as per instructions given and set up by the controller. Effective and efficient training of a model from a limited amount of data is a major limitation of the IoT-Cloud Service Framework for M2M models. Most of the IoT-Cloud Service Framework models in M2M deal with different security purposes and in the medical field like

Medical emergencies, IoT-based devices providing virtual assistance to doctors, and providing information regarding the current condition of patients. Four scenarios can take place for communication:

i) IoT-to-user communication service (when a user wants to check the status of IoT devices)
ii) cloud-to-user communication service (when a user wants to access data of cloud storage)
iii) IoT-to-cloud communication service (when IoT devices want to send their data in cloud storage)
iv) Cloud-to-IoT communication service (when cloud storage wants to synchronize data according to IoT devices)

All of the above four stages are managed by the master controller and have a responsibility to decide traffic flow and data entries of a user, IoT devices, and cloud (both main cloud and Fog cloud). Whenever a node wants to send traffic to any other network node then it has to first establish its connection with the master controller through an IP address. Further, the controller asks for the key from the sender node and when the sender node sends back its key then the controller matches the IP address and key within its table. If both IP address and a private key are within the table then the requested IP address is allowed to access and send its data towards the destination. When data reaches its destination then the destination node also verifies it through its private key and if the key matches then it can utilize the data packet as by instructions of the sender.

Fig. 4 depicts the working of proposed system when an attacker tries to reach and establish a connection within network. In this case, cloud systems contain bogus data files within their storage system and the eavesdropper tries to access data and status of IoT and cloud systems.

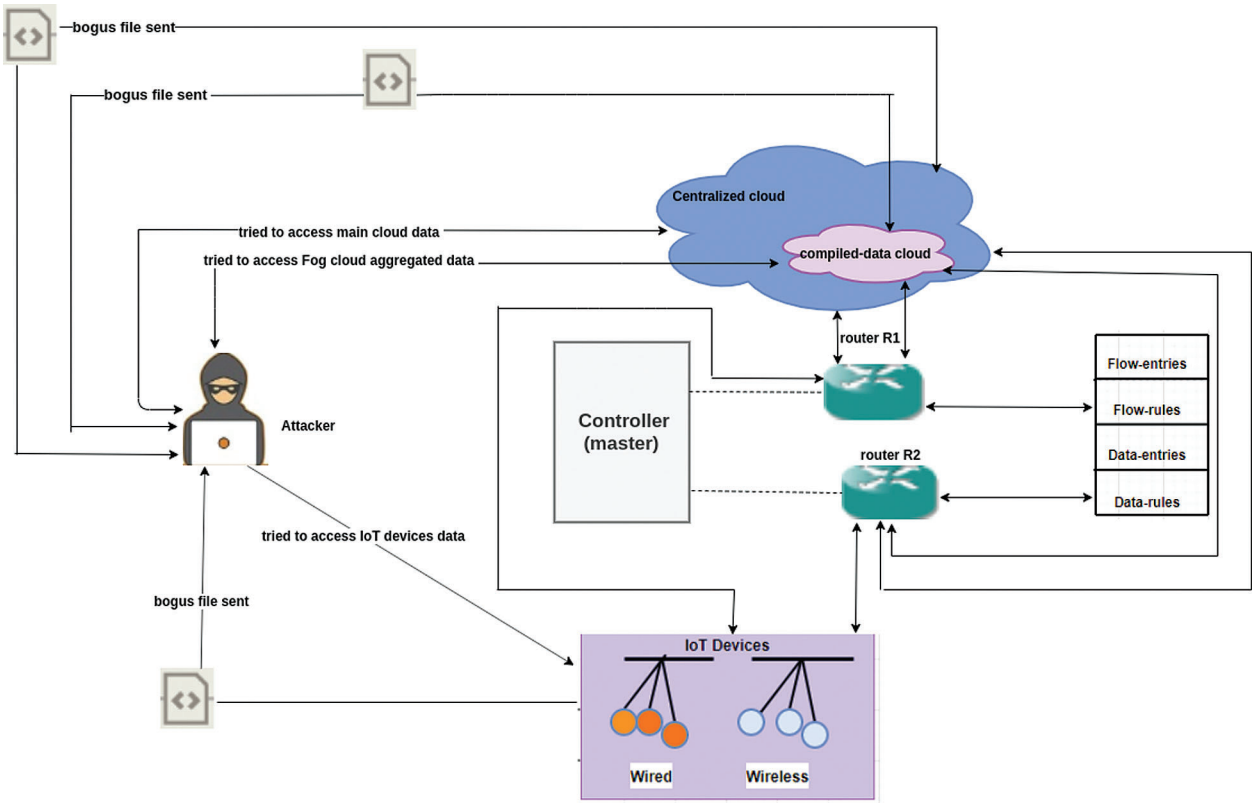

Figure 4: IoT-cloud model for prevention from data access

The controller will matche the IP address and key of the eavesdropper system and when it does not match the controller asks the cloud to send the generated bogus file towards the attacker and on the other side, when an attacker wants to check the status of IoT devices then the controller sends a request to the centralized cloud to send a bogus status file to IoT nodes. Then these nodes send bogus status towards the attacker. In both these scenarios, an attacker thinks that he has successfully breached actual data but in actual he has been given a bogus file as shown in Fig. 4.

4 Security Concerns for Cloud-IoT Modelling

4.1 Network Level Attacks

Security issues are the major issue of cloud computing as hackers, crackers, and security scientists, researchers, and investigators have shown that this prototype is ambiguous and is not guaranteed in cloud systems. In a cloud environment, security is being shared between cloud providers and their users, and both are required to believe each other, wherever there must be a scope of improving security concerns. There are vast kind of security threats, that is why providers have to ensure to their customers regarding transparency of the data, but in case if they fail in securing data this results in inside and outside threats or malicious attacks, data loss, software threats, multi-tenancy threats, Loss of control and Flood attacks [14].

4.1.1 Data Protection

It is one of the major issues of the user while accessing cloud services. It is always the top priority of the user and service provider. Data needs to be protected from unauthorized access and also secure the personal information of users.

4.1.2 Multi-Tenancy Issues

Cloud is mainly intended to assist numerous users, it points towards diverse users within a cloud who share the applications and the physical hardware to run their Virtual Machines (VMs) in PaaS environment. In this scenario, users act as tenants for the provider. While this model looks to be very capable from the provider's perception, it encompasses some thoughtful restrictions in relationships of security. The application and hardware allocation can allow data outflow and misuse and it supports growing the attack surface.

4.1.3 Loss of Control

When cloud providers move data within the cloud, it becomes transparent to them but when organizations send data to the cloud they don't know about its location so in that case, they may lose control of their data. Organizations may not be conscious of any security mechanism laid in place by the provider. So these reasons create a sense of insecurity among clients.

4.1.4 Flood Attacks

Flooding is the denial of service (DOS) attack that affects the performance of the server and makes it unavailable for client requests in cloud environment. An attacker creates a wrong scenario and sends it to the server to make it busy in performing calculations to solve the query request. The worst part of Flood attacks is that they get nasty, it gets stronger because servers use computational power to solve the query thus making it stronger.

4.2 Application-Level Attacks

4.2.1 Inside Threats

It is a recognized fact that insider threats are the most vulnerable threats even with the most progressive firewalls and computer security available to your organizations. If your employees are not trustworthy,

neither can your general security. It is very significant for a company to keep a good sense of direction and management (governance). Some external clients find it more secure to store their data which is suitable to their business at cloud hosting sites. In case, any member (inside threats) among your workforce manages to misapply this data, your cloud company will build a very immoral status about the level of security presented and surely slack existing and forthcoming customers.

4.2.2 Data Loss

Some companies hand over their information to the cloud, which they assume to have a similar level of integrity and protection of data as they would in their locations and geographical area. Data loss and its outflow can root financial loss, bad repute, and buyer count damage to the organization. Erasure or modification of records lacking a backup of the normal content is a recognized example of data loss.

4.2.3 Software Threats

Software is set of programs inscribed by all types of people and some software is required to purchase for use and some are free. Freeware software is generally open-source software, so a developer or a hacker can enter its code, find bugs in it, and can harm the system by this software. These pinpoints are also known as soft targets. Soft targets are usually found on those machines which have Public IPs to connect to the outside world and an eavesdropper can access their data through software and can harm them.

4.2.4 Insecure APIs

Users mainly interact with the interface of the cloud environment. API's are accessible from anywhere, so attackers can use interfaces to compromise the confidentiality of clients. The attacker uses the same token which is given to the user and by using that token the attacker can access their data.

4.2.5 Service/Account Hijack

In an account of hijack the intruder uses the stolen credentials to hijack cloud service and can insert false information, and divert users to fake websites. There is a watering hole attack through which attackers include the malicious code into a webpage to attack the users that visit the website. Attackers can also disrupt the service and make it inaccessible.

4.2.6 Data Security Issues

Data security can be measured in terms of management, migration, and virtualization. For the cloud, data is stored in several places in the back end so this strategy makes the security difficult to manage. In turn, moving data across locations can also have security concerns. Data management security would be considerable in terms of how to deal with unreasonable data structure and the strategy to solve out non-functional data. Cloud provides a virtual environment to perform the task to get the desired results. Virtualization also makes the cloud environment more insecure because the network is complex and this system has to manage properly.

5 Empirical Results

In the above pictorial representation, there are different keywords used to access information about specific frameworks to manipulate and find out methodologies implemented on these countersigns. Likewise, IoT is a big and advanced field taking a very diverse ecosystem as well as Cloud is also taking a large amount of boundary in IT concerning M2M communication as shown in Fig. 5. So these are the identifications to find research papers related to these fields that what terminologies they have used to fulfill real-time applications. While filtering all these parameters many papers have been found related to the medical environment to fulfill the M2M communication approach after finding we also started to find secure connections so there shouldn't be outside threats and attacks.

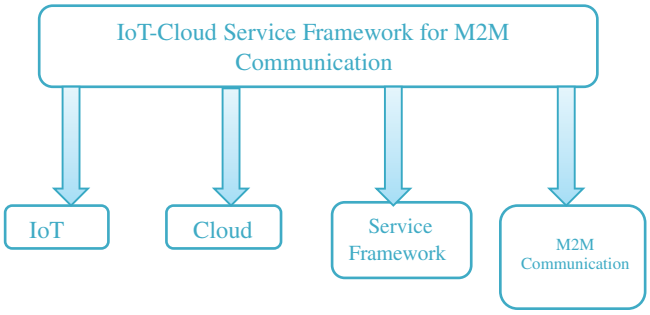

Figure 5: Categories of data access

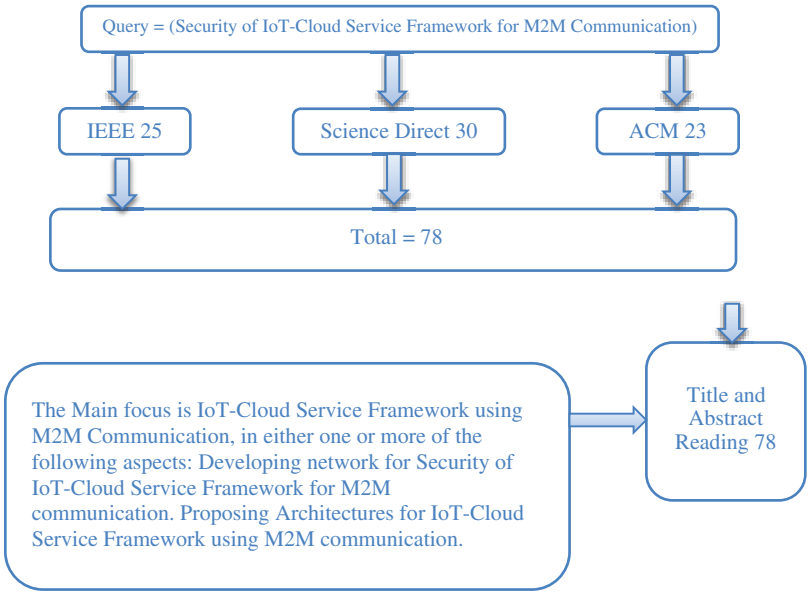

Figure 6: Qualitative data of M2M query

Several models have been used in IoT-Cloud Service Framework for M2M Communication but most of them were medically based. In Medical emergencies, IoT-based devices providing virtual assistance to doctors to provide information regarding the identification of patients. IoT We-Care system for elderly people's health, IoT-based device and it provides virtual assistance to doctors, IoT Smart Home, smart classrooms, eco-friendly solid waste management, agriculture with the use of IoT, smart health system for people with disabilities. Query result of security of IoT cloud service framework for M2M results in 25 papers in IEEE, 30 papers in science direct, and 23 papers in ACM. Total 78 papers title and abstract reading are helpful to formulate the proposed frameworks as shown in Fig. 6.

6 Conclusion

Different studies constituted the synchronized consequences, many of them the latest, presenting a wide-ranging selection of IoT-Cloud Service Framework for M2M Communication. After analyzing and critical study, it found that M2M Models have replaced traditional models used in medical. The M2M-based models give an efficient performance in the medical field as compared to work on general society. Several models have been used in IoT-Cloud Service Framework for M2M Communication. The Internet of Things (IoT) is a framework that allows everyday things to become smarter, processing to become

more intelligent, and communication to become more informative. The conformation of associated fields is always paved by specialized architectural studies. Researchers are now struggling to get through the scope of Internet of Things-centric techniques due to a lack of comprehensive architectural expertise..

Acknowledgement: Thanks to our families and colleagues, who provided moral support.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Botta, D. Donato, W. Persico and V. Pescapé, "Integration of cloud computing and internet of things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[2] A. Bouguettaya, "From IoT data to services," in *Proc. of 2018 Int. Symp. on Programming and Systems (ISPS)*, Algeria, no. 34, pp. 1–1, 2018.

[3] H. Cai, B. Xu, B. Jiang and L. Vasilakos, "Iot-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 75–87, 2017.

[4] D. Costa, K. A. Papa, P. Lisboa, C. Munoz and C. Albuquerque, "Internet of things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[5] G. Arani, M. Jabbehdari and S. Pourmina, "An autonomic resource provisioning approach for service-based cloud applications: A hybrid approach," *Future Generation Computer Systems*, vol. 78, pp. 191–210, 2019.

[6] J. Hong, A. Nhlabatsi, D. Kim, N. Fetais and M. Khan, "Systematic identification of threats in the cloud: A survey," *Computer Networks*, vol. 150, pp. 46–69, 2019.

[7] S. Mohanty, P. Choppali and E. Kougianos, "Everything you wanted to know about smart cities: The internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 3, no. 5, pp. 60–70, 2019.

[8] S. Naz, S. Abbas, M. Adnan, M. Abid, B. Tariq *et al.*, "Efficient load balancing in cloud computing using multi-layered mamdani fuzzy inference expert system," *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 10, pp. 569–577, 2019.

[9] G. Neagu, S. Preda, A. Stanciu and V. Florian, "A cloud-IoT based sensing service for health monitoring," in *Proc. of the 2017 E-Health and Bioengineering Conf.,* Sinaia, Romania, *EHB 2017*, pp. 53–56, 2017.

[10] R. Neupane, L. Neely, P. Calyam and R. Durairajan, "Intelligent defense using pretense against targeted attacks in cloud platforms," *Future Generation Computer Systems*, vol. 93, no. 5, pp. 609–626, 2018.

[11] I. Priya, P. Pathak and A. Tripathi, "Big data, cloud and IoT: An assimilation," in *Proc. of 2018 2nd Int. Conf. on Advances in Computing, Control and Communication Technology, IAC3T 2018*, Allahabad, India, pp. 34–40, 2018.

[12] M. Aslanpour, M. Ghobaei and A. Nadjaran, "Auto-scaling web applications in clouds: A cost-aware approach," *Journal Network Computer Application*, vol. 95, pp. 26–41, 2017.

[13] W. Yu, W. Dillon, T. Mostafa, F. Rahayu and W. Liu, "A global manufacturing big data ecosystem for fault detection in predictive maintenance," *IEEE Transactions on Industrial Informatics*, vol. 23, pp. 1–1, 2019.

[14] J. Zhou, Z. Cao, X. Dong and V. Vasilakos, "Security and privacy for cloud-based iot: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.