EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

An analysis of security challenges and their perspective solutions for cloud computing and IoT

Muhammad Hassan Ghulam Muhammad[1], Tahir Alyas[1,*], Faraz Ahmad[1], Fatima Hassan Butt[2], Wajahat Mahmood Qazi[3], Shazia Saqib[1]

[1] Department of Computer Science, Lahore Garrison University, Lahore, Pakistan
[2] Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan
[3] Department of Computer Science Comsats University Islamabad, Lahore Campus, Pakistan

Abstract

INTRODUCTION: With the on-going revolution in the Internet of Things and Cloud Computing has made the potential of every object that is connected through the Internet, to exchange and transfer data. Various users perceive this connection and interaction very helpful and serviceable in their daily routines.
OBJECTIVES: The objective of this research to identify the complex configured network system is a soft target to security threats, therefore we need a security embedded framework for IoT and cloud communication models. Another objective is to provide protection of information from unauthorized access controls in IoT-cloud integrated framework and secure data from spying.
METHODS: This paper has applied an integrated IoT-cloud theoretical solution, whose activities are mainly decided by a centralized controller to provide safeguard against data attacks. Our theoretical integrated IoT-cloud theoretical solution is able to achieve unauthorized access control and data breach.
RESULTS: Internet of things and cloud computing has intensively used by several real-time applications. After the thercical analysis, the different vulnerabilities explained after detail literature review to prevent unauthorized access and unauthorized data breach.
CONCLUSION: Internet of things have changed the shape of communication and centralized data controller is the main entity that is robust against eavesdroppers. In case, any eavesdropper tries to be a normal user and attempts to access a personal file then he has been entertained with a misleading file that he considers as an authentic file but in actual it is not. Desirable IoT proposed solutions need to be design and deploy, which can guarantee: anonymity, confidentiality, and integrity in heterogeneous environments.

Keywords: Cloud Computing, Cloud Security, Internet-of-Things, Denial of service
Received on 29 June 2020, accepted on 27 September 2020, published on 23 October 2020

doi: 10.4108/eai.23-10-2020.166718
*Corresponding author. Email: tahiralyas@lgu.edu.pk

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 are being considered as the imperative topics researched globally, so the Internet of things (IoT) 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. Additionally, their emerging trends have increased the value in 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 that 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. On

the cloud side, many other devices have also been connected and exchanging information about data records of medical machines and other electrical appliances.

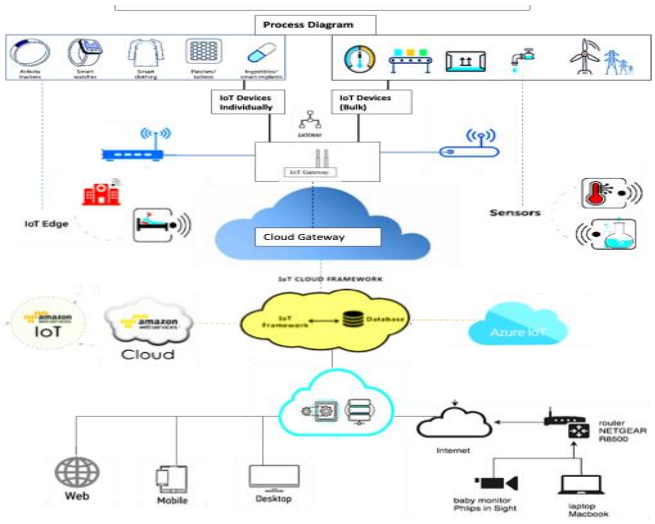

Figure 1. IoT and Cloud integration

From a security perspective, the immense amount of data produced by IoT devices [2] and stored on cloud storage is flooding the world with security disasters. Moreover, independent IoT devices are not protected at all, thus easily exploited by various families of attacks. IoT devices used as lightweight devices are supported by the cloud as these devices store their collected and processed data on cloud servers. The huge amount of data sent towards the cloud makes IoT devices dependent on cloud storage. In this paper is to investigate and work on such a framework that can prevent unauthorized data breaches on both IoT and cloud sides.

IoT and cloud as two different entities, has changed the shape of computing wold and added their updated and well-structured security issues. The outcome of the related work summary explained how IoT and cloud usage has affected modern society. The main focus is to deal with unauthorized access controls in IoT-cloud integrated framework and prevent sensitive and confidential data to be accessed by a spy or attacker.The major focus is on the Internet of Things and cloud Integration that is genuinely a productive field on both industries as well as research platforms that show a promising attitude towards the diaphragm who are currently merchandising IoT and cloud.

1.1. IoT Being a Network of Networks

Currently, IoT consists of a loose collection of disparate, purpose-built networks. 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 others, will relate to added security, analytics, and Fig.2 management capabilities. This will enable IoT to turn into even more capable and powerful in what it can help individuals to accomplish [4,5].

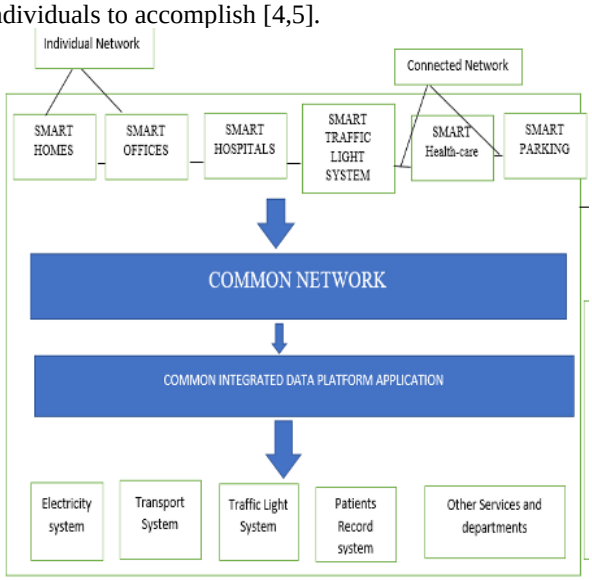

Figure 2. IoT services and applications

2. Cloud computing

Cloud computing is a hosted service provided over the internet. It provides high performance

The 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 you can access data

2.1. Paradigms of Cloud computing

There are four ways to develop a cloud computing environment and each one has its security concerns. Public cloud, Private cloud, community cloud, and hybrid cloud [6]

2.1.1. Public Cloud

Public clouds are operated and maintained by cloud service providers. Any client can use these services through a web browser. Data is stored in the service provider's data center and the provider is accountable for the management and maintenance of data.

2.1.2. Private Cloud

Private clouds are maintained by a single organization and company. Only authenticated users can get access to data in these clouds. These data centers are protected as compared to public clouds.

2.1.3. Hybrid Cloud

Hybrid clouds used the infrastructure and services of public and private clouds. These clouds use secure services from private clouds and non-sensitive services from public clouds. As compared to public and private clouds hybrid cloud provides businesses with better elasticity and more deployment opportunities.

2.1.4. Community Cloud

Community cloud computing provides a shared cloud service environment that facilitates a limited set of organizations or employees. This cloud is managed by participating organizations or service providers to achieve specific goals and work in joint projects. It provides the ability to easily share and collaborate at a lower cost.

2.2. Cloud Service Models

Organizations develop or adopt any cloud environment according to their requirement. The following are the three basic cloud service model.

2.2.1. Infrastructure as a service

IaaS is the basic layer in cloud computing models that provide the infrastructure of the cloud. It is also known as a layer of computing and required changes when new requirements take place and have to re-design from bottom to top. Work on a hardware level and change according to their desired structure, and deal with network and storage resources considered as virtual resources but these changes are on temporary basics and designed for a specific task to perform.

2.2.2. Platform as a service

PaaS is a cloud service that offers a platform to develop software on which users can run code and check whether it's according to their needs or requirements. It could be interaction with programming languages used to achieve specific purposes dealing with databases, web servers, and file storage but without the management at a lower level.

2.2.3. Software as a service

SaaS is a service that provides software solutions to clients so they can use them according to their requirements. The client doesn't have access to either to do any kind of software change or to deal with its infrastructure, but only to use its services is the author to whom proofs of the paper will be sent.

3. Security Concerns of IoT

Even though IoT has made technological advances, it has been widely recognized that security has become a major concern that seriously has affected the successful deployment and development of an IoT infrastructure [8]. Now we have explained various security attacks that have a great concern in the IoT environment [9].

3.1. Physical Attacks

These attacks occur when an attacker is physically nearer to a network system. The few common classifications of these attacks are listed below:

3.1.1. Sleep Denial Attack

This attack mainly harms the battery power of a device by feeding false inputs to that device. it results in the shutting down of the device because of over-exhaustion.

3.1.2. Permanent Denial of Service

This attack launches a corrupted BIOS, on IoT devices with the help of malware.

3.1.3. Fake Node Injection

An attacker launches a fake node between two nodes to disrupt and lead the communication between two legitimate nodes.

3.2. Network Attacks

These attacks damage the IoT network system [11] and few classifications of these attacks are listed below:

3.2.1. Traffic Analysis Attack

Such attacks cause harm to gain information on IoT networks. An attacker tries to breach the confidential information that is flowing to and from devices and an attacker can try to breach this information without going closer to that particular network [12].

3.2.2. Selective Forwarding

In this attack, a malicious node becomes part of a network and sends, alters, or drops a message to another node within the network [13].

3.2.3. Distributed Denial of Service Attack

Multiple compromised nodes attack a particular node by over-flowing messages or connection requests and that will result in slow down or even crash a whole network [14].

3.3. Software Attacks

Attacks in which an attacker tries to take advantage of associated software or any other security vulnerability that is part of an IoT system and those attacks. Data of IoT devices are attacked by malware which can further contaminate the cloud. Cloud user unknowingly uses this software then it can alter or even steal information of IoT devices[15].

3.4. Data Attacks

Such attacks in which an attacker tries to breach and alter the data of an IoT device.

3.4.1. Unauthorized Access

Such attacks in which an attacker becomes an authorized member and gains ownership rights of sensitive data.

3.4.2. Data Breach

Data breach is a type of security incident, that can result in personal or business information is accessed without authorization. Data breaches can result in a great lose of personal and business in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair. Data breach attack can result in the leak of personal, sensitive, and confidential information.

4. Security Concerns in Cloud System

Security issues are the core issue of cloud computing as hackers, crackers, and security scientists, researchers, and investigators have shown that this prototype is ambiguous and is not 100% guaranteed. In a cloud environment, security is being shared between cloud providers and its 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 the 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, Flood attacks, etc.[19].

4.1. Insider 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 PC. 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 clienteles find it more secure to store their data which is subtle to their business at cloud hosting sites. In case, any member 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 [20].

4.2. Data loss

Some companies hand over their information to the cloud, they assume to have a similar level of integrity and protection of data as they would in their locations. Data injury 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 novel content is a recognized example of data loss [21].

4.3. Software threats

Software is programs inscribed by all types of people and some software 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 usually found on those machines which have Public IP's to connect to the outside world and an eavesdropper can access their software and can harm them [22].

4.4. Multi-Tenancy Issues

Cloud is mainly intended to assist numerous users; it points towards diverse users within a cloud that share the applications and the physical hardware to run their Virtual Machines (VMs). In this scenario, users act as tenants for the provider. While this model looks to be very capable of 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 [23].

4.5. Loss of control

When 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 [23].

4.6. Flood attacks

Flooding is the denial of service attack which affects the performance of the server and makes it unavailable for client requests. An attacker creates a wrong scenario and sends it to the server to make it busy in performing calculations to solve the query. The worst part of Flood attacks is they get nasty, it gets stronger because servers use computational power to solve the query thus making it stronger [24].

4.7. Data Protection

It is one of the major issues of the user while using cloud services. It is always on 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 [25].

4.8. Insecure APIs

Users mainly interact with the interface of the cloud environment. APIs are accessible from anywhere, so attackers can use interfaces to compromise the confidentiality of clients. Attackers use the same token which is given to the user and by using that token the attacker can access their data [26].

4.9. Service/Account Hijack

In account hijack, the intruder uses the stolen credentials to hijack cloud service and can insert false information and divert users to abuse 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 [27].

4.10. 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 dig 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 be managed in a proper manner [28].

5. Impact of IoT Models on Society

In this section different IoT implemented systems will be discussed and that will tell how authors mentions reason for comfort for people and when people are at ease, the overall society will be at ease.

S. Pinto et al. [29] 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 (e.g. it can detect falls).

Kajal R.K Pandey et al. [30] proposed model works in 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 the medical information of every victim. This dedicated device is a wearable identity which has a unique identification number.

Shilpa Mandke et al. [31] 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 his pulse rate. This model is designed by keeping in mind mothers of 3rd world countries, when they are away from their new-borns or out from home for the sake of work. This system is composed of Temperature sensors, pulse sensors, a voice sensor, a motion sensor, and these sensors give information to microcontrollers. This microcontroller is also attached to a power supply and a Wi-Fi module. And Wi-Fi modules with the help of the internet send information to a database of a mother's phone or laptop or any device which is part of this system.

Asim Majeed et al. [32] works for 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.

J Arora et al. [33] 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.

A Khan et al. [34] also proposed a smart home called as an IoT Smart Home System (IoTSHS) which consist of the 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.

BS Singh et al. [35] proposed a smart health system for people with disabilities. This paper proposes some components (RFID sensor which will give direction to blind people, camera, sensors for impaired people ear, wireless glove) to help and improve the lifestyle of handicapped people.

Y Zang et al. [36] worked on two-hop wireless communication for collecting IoT data under eavesdropper collusion in which researchers adopted physical layer security to prevent such attacks. Also, researchers worked on two cases: in the first case, eavesdropper worked independently and in the second case M observation of eavesdroppers are combined to conduct an eavesdropping attack. They indicated that eavesdropper collusion can increase secrecy outrage and can drop the security performance of IoT data collection. Additionally, authors have proposed that cooperative jamming schemes can help to improve data collection security either by increased noise generated threshold or by distributing more relays.

Table 1. IoT Based Models with their Impact on Society

Authors	Smart System	Proposed For
S. Pinto et al.	We- Care Model	Elderly people and patients
KAajal R.K Pandey	Virtual assistance Model	Victims in emergency
Shilpa Mandke et al.	Infant Health Monitoring System	Keeps track of infant parameters like pulse rate, their movement as well
Asim Majeed et al.	Smart Classroom Model	Smart Education System
BS Singh et al	Smart Health System for People with Disabilities	Improve the lifestyle of Handicap
Khan et al.	Smart Home	Operate home appliances with infrared remote
Arora et al.	Smart Home	Keep track of different and critical parameters of the home

6. Impact of Cloud on Society

In this section, detailed literature review is discussed how cloud computing has worked to improve the quality of life around us.

Mhouti et al. [38] have discussed cloud computing services for e-learning systems which can benefit higher education institutions. These cloud computing services can be used anytime, anywhere as well as lower software and hardware requirements.

Basha et al. [39] discussed that cloud computing is a pillar of e-learning as it helps instructors and students to access new knowledge.

Tuli et al. [40] proposed a Robust Weibull model based on iterative weighting that has combined cloud computing and machine learning together to predict the epidemic growth of COVID-19.

MA Khasawneh et al. [41] discussed that cloud computing has a great impact on the growth of green supply chain management, for example, improved information availability, which is an important factor for energy saving, improved dealing speed with information, reduced cost of running, etc.

I Singh et al. [42] proposed an e-health administration framework in which patient data is supposed to be filled in the database. There is a web-empowered system on the cloud side which consists of specialists, radiologists, and research center staff. This proposed architecture data is also secured with biometric authentication agents and authenticating user access.

Table 2. Cloud Computing Based Models with their Impact on Society

Authors	Cloud-Based System	Proposed For
A El Mhouti et al.	e-learning system	To benefit higher education
D Basha et al.	e-learning system	To facilitate instructors and students
S Tuli et al.	Robust Weibull model	To predict the growth of COVID-19
MA Khasawneh et al.	Green supply chain management	To improve the traditional supply chain management system
J Wei et al	Integrated model cultural platforms in china	Improved cultural platforms, smart individual spaces, and physical cultural venues.
P Sing et al.	Smart monitoring and controlling of government policies	Improved policymaking for government
I Singh et al.	e-health administration framework	To facilitate patients with web empowered system

P Sing et al. [43] has worked on smart monitoring and controlling government policies with the help of cloud computing and social media. Authors have tested their approach on Goods and Services Tax by the Indian government and results showed that their proposed pragmatic approach is a feasible choice for efficient policymaking and its implementation.

J Wei et al. [44] have proposed a theoretical integration model for cloud-based cultural platforms in china. This paper has also worked on improving the interaction between cloud-based cultural platforms, smart individual spaces, and physical cultural venues.

B EL Zoghbi et al. [45] discussed that traditional IT and related IT service provider roles are affected by Cloud computing technology in Lebanon. Authors have used a qualitative interpretive multiple case study approach and discussed CC value co-creation opportunity for IT service providers in Lebanon that identified their modern role in fixing the Cloud Computing roadmap from a service-dominant logic.

K Cheng et al. [46] have proposed a novel scheme for a secure k-NN queries on encrypted cloud data with multiple keys to provide confidentiality and privacy for data. In this scheme, DO and each QU all hold their different keys, and they do not share them. Meanwhile, the DO is responsible to encrypt and decrypt outsourced data with the help of his key. Also, researchers have constructed their scheme using a distributed two trapdoors: public-key cryptosystem (DT-PKC) and a set of protocols of secure two-party computation, which are responsible to preserve the data confidentiality, query privacy, and offline data owner.

E Kabir et al. [47] presented a sorting framework for Statistical Disclosure Control (SDC) which helps to protect microdata in cloud computing. This framework of two stages: in the first stage, an algorithm sorted all records in a particular way which ensured that dissimilar observations do not enter in the same cluster, and the second stage a microaggregation method is used by authors to create k-anonymous clusters while reducing the information loss.

H Wang et al. [48] have combined cryptography with authorizations in their proposed work. Also, authors have assigned keys to data owners to roles that will enforce access via encryption. Additionally, a formal access model is designed which analyzes the translating an authorization policy into an equivalent encryption policy. The authors have also investigated the effect of role hierarchy structure in the authorization process. The role-based access management methods are implemented with *XACML* by using *WSO* Identity Server.

7. Suggested Integrated Solution of IoT-Cloud security Concerns

After detailed related work, Structure for the secure integration of an IoT computing devices with cloud systems is proposed. Interconnected cloud and IoT devices with a centralized controller as shown in Fig.3. to examine security controls that can be used to secure IoT system data and cloud data. Therefore, the ubiquitous access to different types of information would be allowed through proposed centralized controllers which will help in terms of the 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.

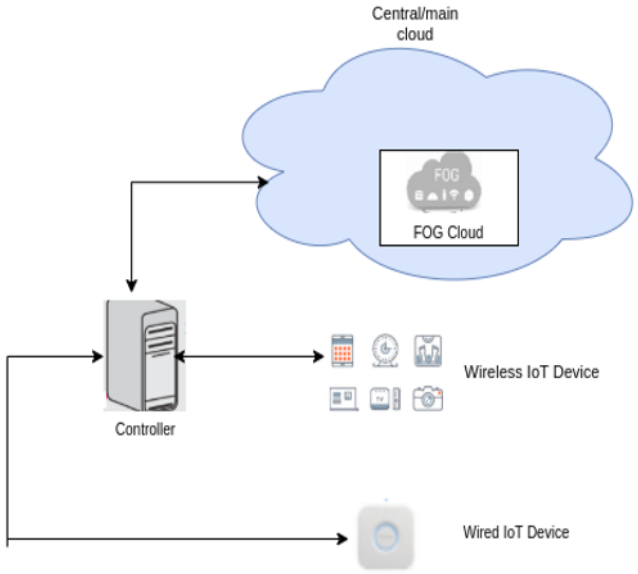

Figure 3. IoT-Cloud Integrated model

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 attacks 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.

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 by instructions given and set up by the controller.

The following four scenarios can take place for communication:

(i) IoT-to-user communication service (when a userwants to check the status of IoT devices).

(ii) cloud-to-user communication service (when auser 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 4 stages are managed by the master controller and have the responsibility to decide traffic flow and data entries of the user, IoT devices, and cloud both main cloud and Fog cloud.

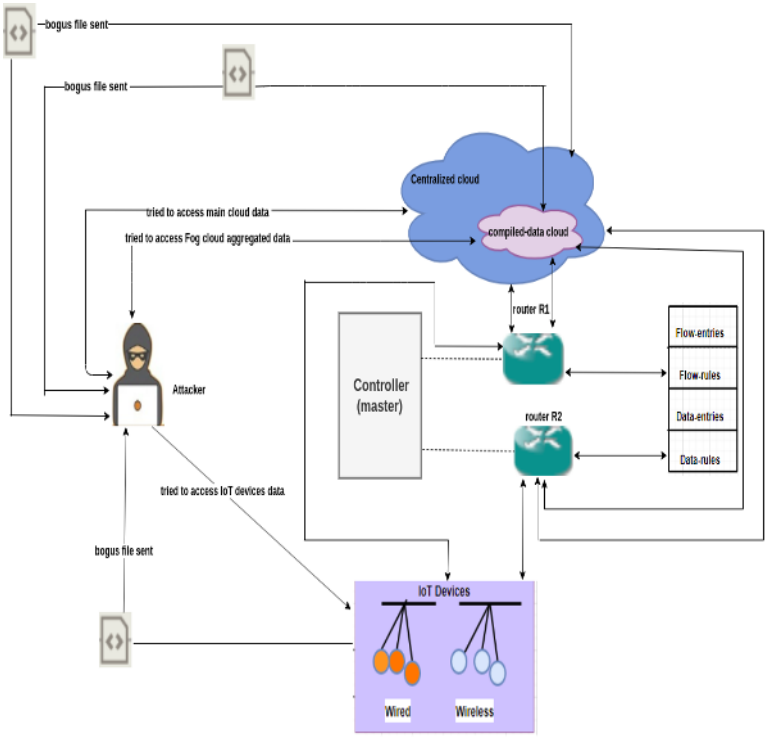

Figure 4. IoT-Cloud Secure model

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 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 the IP address and the 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 than 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.

In this case, cloud systems contain bogus data files within its storage system. When an eavesdropper tries to access data and status of IoT and cloud systems then it first has to go through a controller. The controller matches 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

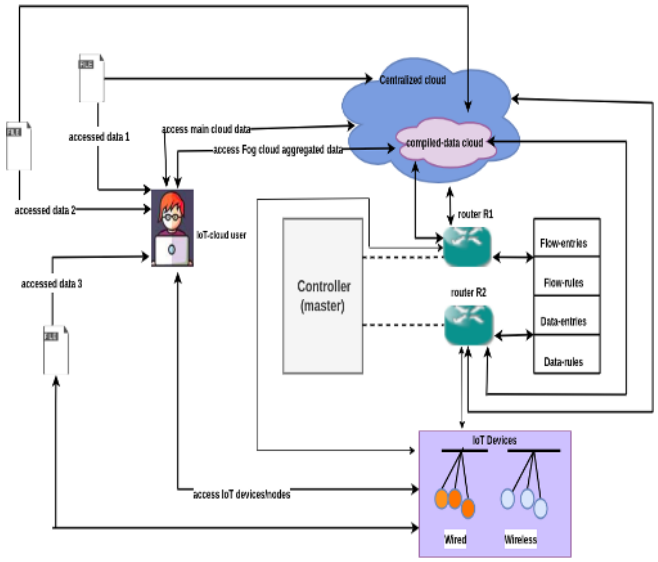

Figure 5. IoT-Cloud prevention Model from data access

On the other side, when an attacker wants to check the status of IoT devices then the controller sends a request to the controller 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.

Conclusion

IoT and cloud computing have been intensively used by several real-time applications. To prevent unauthorized access and unauthorized data breach, an IoT-cloud communication model is proposed. Different cases with centralized controller that control the main entity that is robust against eavesdroppers. Any data breaches eavesdropper tries to be a normal user and attempts to access a personal data is identified through proposed model and can misleading the attack.

References

[1] Ray, P. P. A survey of IoT cloud platforms. Future Computing and Informatics Journal. 2016; 1(1-2): 35-46.

[2] De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., Mazzara, M. Cyber-storms come from clouds: Security of cloud computing in the IoT era. Future Internet. 2019; 11(6): 127.

[3] Rajendran, G., Nivash, R. R., Parthy, P. P., Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures.In International Carnahan Conference on Security Technology (ICCST); IEEE; 2019. p. 1-6.

[4] Sengupta, J., Ruj, S., & Bit, S. D.A Comprehensive survey on attacks, security issues, and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications. 2020; 149: 102481.

[5] Kafle, V. P., Fukushima, Y., Harai, H.Internet of things standardization in ITU and prospective networking technologies. IEEE Communications Magazine.2016.54(9):43-49.

[6] Velte, A. T., Velte, T. J., Elsenpeter, R. C., Elsenpeter, R. C. Cloud computing: a practical approach. New York: McGraw-Hil (ISBN-13:978-0-07-068351-8); 2010. p. 1-55.

[7] Marinescu, D. C. Cloud computing: theory and practice. Morgan Kaufmann; 2017.

[8] Wang, H., Zhang, Z., Taleb, T. Special issue on security and privacy of IoT. World Wide Web. 2018; 21(1):1-6.

[9] Atlam, H. F., Wills, G. B.IoT security, privacy, safety and ethics. In Digital Twin Technologies and Smart Cities.Springer, Cham;2020. p. 123-149.

[10] Alladi, T., Chamola, V., Sikdar, B., Choo, K. K. R. Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine. 2020; 9(2): 17-25.

[11] Sengupta, J., Ruj, S., Bit, S. D. A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications. 2020; 149(102481).

[12] Andrea, I., Chrysostomou, C., and Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges, In: *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, doi: 10.1109/ISCC.2015.7405513, 2015, 180-187.

[13] Varga, P., Plosz, S., Soos, G., and Hegedus, C. Security threats and issues in automation IoT. In: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, Trondheim, doi: 10.1109/WFCS.2017.7991968,2017, 1-6.

[14] Wang, B., Zheng, Y., Lou, W., and Hou, Y. T. DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks* Vol.81 (2015) 308-319.

[15] Prasad, R., Rohokale, V. Cyber Threats and Attack Overview. In Cyber Security: The Lifeline of Information and Communication Technology. Springer, Cham.2020;15-31.

[16] Ma, R., Chen, S.,Ma, K., Hu, C., and Wang, X. Defenses against wormhole attacks in wireless sensor networks. In: *International Conference on Network and System Security*. Springer, Cham;2017.

[17] Jesudoss, A., and N. Subramaniam. A survey on authentication attacks and countermeasures in a distributed environment.Indian Journal of Computer Science and Engineering (IJCSE). 2014;5(2): 71-77.

[18] Hou, J., Qu, L., Shi, W. A survey on internet of things security from data perspectives. Computer Networks. 2019;148, 295-306.

[19] Hoogvliet, M. T. SaaS Interface Design. Designing web-based software for business purposes. thesis in Communication and Multimedia Design. 2008.

[20] Dawoud, W., Takouna, I.,Meinel, C. Infrastructure as service security: Challenges and solutions. In: 7th International conference on Informatics and Systems (INFOS), IEEE; 2010.p. 1-8.

[21] Yan, C. Cybercrime forensic system in cloud computing. In Proceedings of 2011 International Conference on Image Analysis and Signal Processing, IASP; 2011.p. 612-3.

[22] Nayyar, A.Private Virtual Infrastructure (PVI) Model for Cloud Computing. International Journal of Software Engineering Research and Practices,2011; 1(1): 5.

[23] Sosinsky, B. cloud computing bible.John Wiley & Sons.2010;762.

[24] You, P., Peng, Y., Liu, W., amp; Xue, S.Security issues and solutions in cloud computing. In Distributed Computing Systems Workshops (ICDCSW), IEEE. 2012. P.573-577.

[25] Behl, A. Emerging security challenges in cloud computing: An insight into cloud security challenges and their mitigation.In:2011 World Congress on Information and Communication Technologies(WICT),IEEE;2011. 217-222.

[26] Krutz, R. L., amp; Vines, R. D. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.2010.

[27] Zissis, D., amp; Lekkas, D. Addressing cloud computing security issues. Future Generation computer systems.2012;28(3): 583-592.

[28] Chaitin, G. J.Information, randomness & incompleteness: papers on algorithmic information theory.World Scientific.1990;8.

[29] Pinto, S., Cabral, J., amp; Gomes, T. We-care: An IoT-based health care system for elderly people. In Industrial Technology (ICIT). In:2017 IEEE International Conference on,IEEE; 2017.p.1378-1383.

[30] Pandey, K. R., Arwat, K., Sharma, I., amp; Patil, S. Improvement and Enhancement in Emergency Medical Services using IOT.2018.

[31] Mandke, S., Kudave, K., Labde, R., amp; Bakal, P. D. J. IOT based Infant Health Monitoring System.2018.

[32] Majeed, A., amp; Ali, M.How Internet-of-Things (IoT) making the university campuses smart? QA higher education (QAHE) perspective. In Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual; IEEE; 2018,p. 646-648.

[33] Arora, J., amp; Kumar, R. IoT-Based Smart Home Systems. In Innovations in Computer Science and Engineering.Springer, Singapore. 2019;531-538.

[34] Khan, A., Al-Zahrani, A., Al-Harbi, S., Al- Nashri, S., amp; Khan, I. A.Design of an IoT smart home system. In: Learning and Technology Conference (L&T),IEEE; 2018;p. 1-5.

[35] Singh, B. S.IOT based Smart Healthcare Applications for People with Disabilities. ASIAN JOURNAL FOR CONVERGENCE IN TECHNOLOGY (AJCT)-UGC LISTED. 2018;4(I).

[36] Zhang, Y., Shen, Y., Wang, H., Yong, J., and Jiang, X. On secure wireless communications for IoT under eavesdropper collusion. *IEEE Transactions on Automation Science and Engineering*, Vol.13 (No.3) (2015) 1281-1293.

[37] Shen, Y., Zhang, T., Wang, Y., Wang, H., and Jiang, X. Microthings: A generic iot architecture for flexible data aggregation and scalable service cooperation. *IEEE Communications Magazine*, Vol.*55*(No.9) (2017) 86-93.

[38] El Mhouti, A., amp; Erradi, M. Harnessing Cloud Computing Services for E-Learning Systems in Higher Education: Impact and Effects. International Journal of Information and Communication Technology Education (IJICTE),2019; 15(2):18-30.

[39] Basha, A. D.Cloud Computing Pillar-E- Learning. International Research Journal of Computer Science (IRJCS).2020; 7: 16-20.

[40] Tuli, S., Tuli, S., Tuli, R., amp; Gill, S. S. Predicting the Growth and Trend of COVID-19 Pandemic using Machine Learning and Cloud Computing. Internet of Things.2020;100222.

[41] Khasawneh, M. A. (2020). Impact of Cloud Computing on Green Supply Chain Management. In: Handbook of Research on Interdisciplinary Approaches to Decision Making for Sustainable Supply Chains; ICI Global;2020.p. 476-490.

[42] Singh, I., Kumar, D., amp; Khatri, S. K. Improving The Efficiency of E-Healthcare System Based on Cloud. In: 2019 Amity International Conference on Artificial Intelligence (AICAI);IEEE;2019. p. 930-933.

[43] Singh, P., Dwivedi, Y. K., Kahlon, K. S., Sawhney, R. S., Alalwan, A. A., amp; Rana, N. P. Smart monitoring and controlling of government policies using social media and cloud computing. Information Systems Frontiers.2019; 1-23.

[44] Wei, J.,Wang, Z.How are cloud-based platforms changing cultural services: Towards a new service integration model. *iConference 2020 Proceedings*.2020.

[45] El Zoghbi, B., amp; Chedrawi, C.Cloud Computing and the New Role of IT Service Providers in Lebanon: A Service-Dominant Logic Approach. In: ICT for an Inclusive World;Springer Cham;2020.p. 425-437.

[46] Cheng, K., Wang, L., Shen, Y., Wang, H., Wang, Y., Jiang, X., and Zhong, H. Secure k-nn query on encrypted cloud data with multiple keys. *IEEE Transactions on Big Data*, (2017).

[47] Kabir, E., Mahmood, A., Wang, H., and Mustafa, A. Microaggregation sorting framework for k-anonymity statistical disclosure control in cloud computing. *IEEE Transactions on Cloud Computing*, (2015).

[48] Wang, H., Yi, X., Bertino, E., and Sun, L. Protecting outsourced data in cloud computing through access management. *Concurrency and computation: Practice and Experience*, Vol. *28*(No.3), (2016) 600-615.