International Journal of Data Informatics and Intelligent computing (IJDIIC)
Vol. 2, No. 1, March 2023, pp. 62~69
DOI: 10.59461/ijdiic.v2i1.44

Dynamic Mobile Cloud Eco System Security - A Review

M.Anitha[1], M. Senbagavalli[2]
[1]Department of Computer Science and Engineering, Anna University, Chennai, Tamilnadu, India.
[2]Department of Computer Science and Engineering & Information Technology, Alliance University, Bengaluru, India.

Article Info

Article history:

Received February 24, 2023
Revised March 10, 2023
Accepted March 21, 2023

Keywords:

Mobile Computing
Security and threats
Mobile data protection
Internet of Things

ABSTRACT

Mobile cloud computing is the technique of using cloud technology and various rich mobile applications are intended to be able to run on a variety of mobile devices using the technique called mobile cloud computing. In recent years, huge amounts of data are stored by the clients which are much more easily to the integration of cloud platforms into mobile systems. The ways of security used in portable device settings are one of the key challenges in this respect as the number of people using smartphones continues to rise. None of the models that have been developed with confidence and privacy for precaution of data in mobile cloud systems are impervious to destructive attacks, despite countless attempts. While mobile cloud computing has great potential, security, privacy, viability, and accessibility concerns must still be considered by both consumers and businesses. Additionally, it emphasizes the use of Canny Card Web Services (CCWS) competition to enhance mobile cloud computing security with IOT. This paper has been presented with more than one user application: a smart house and a smart parking in an educational institution, in the inclusion of IOT with cloud computing for demonstrating various admittance control and endorsement requirement. A review regarding this paper concentrated on a little model that is intended the security and privacy ensureability of data in mobile clouds. Additionally, to manage mobile cloud security difficulties and challenges, it is important to look at the current situation with regard to cloud security breaches, the weaknesses of mobile cloud devices, and the best ways to address these issues in the near future with regard to mobile device management and mobile data protection.

Corresponding Author:

M. Senbagavalli
Department of CSE & IT
Alliance University
Bengaluru, India.
Email: senba1983@gmail.com

1. INTRODUCTION

Mobile devices and cloud computing are two key technical advancements that look to have recently. Mobile with cloud is the result of the integration of the provision of powerful computational resources to mobile users is made possible by wireless networks, mobile computing, and cloud computing. Opulent computation assets are readily unfilled, which benefits both network operators and cloud service providers. All the processing and storage capabilities that was previously housed by mobile devices is now switched to more potent and federal platforms found in the cloud to MCC. By using on-demand self-service over the mobile network, it provides a variety of IT resources and information services. By the way of fully utilizing cloud computing, mobile users are given access to new types of services and facilities. Instead of being contained on a single local computer, resources in mobile cloud computing are dispersed among a few virtualized distributed machines. For the benefit of customers and businesses, various businesses supply

several mobile cloud options, such the Google-provided Android operating system. Google has introduced new services like geographic search and Google maps using mobile devices and cloud computing.

A platform with software and services called LiveMess was introduced by Microsoft, allowing users to access and share their data and apps. For the purpose of data backup and storage for apple customers, Apple created iCloud. The hardware limitations of limited calculating power and storage capacity can be overcome via mobile cloud computing, which also enables easy access to data. Internet of Things (IoT) has accelerated significantly in topical years to advances in technology and the Internet. IoT applications and smart IoT devices are multiplying swiftly. These tools and programmes mainly collect, hold, and distribute user data. IoT can use its limitless capabilities, including analytics, compute, and storage, to cloud computing. These days, cloud and IoT are moving in parallel and creating a dynamic cloud-IoT architecture called cloud-enabled Iot.

Numerous technology-enabled services, including bill payment and travel booking, connecting through people, determining one's location, online shopping, and healthcare services, have been made available to users as a result of recent advancements in the communication and Internet industries [1]. Additionally, the Internet of Things (IoT) has assimilated into people's lives and offers convenience in their daily tasks. In the commercial sector, numerous IoT platforms, tools, and applications are being introduced. Most of these platforms are made available by a number of businesses and service providers, each of whom has their own set of standards and operating procedures [2]. In contrast, IoT devices have limited resources and rely on cloud computing for analysis, calculation, and storage [3]. The IOV(Vehicles), canny house, sports and fitness, and healthcare are examples of IOT applications [4]. The vast majority of IOT Mobile devices are used to execute programmes, and vast volumes of data are saved in the cloud. Since processing and findings in real-time is necessary must be made available as soon as practical in the IOT, MCC is extremely helpful (IOT) [5].

The expansive IoT data that is continuously produced, consumed, and distributed is at considerable danger of isolation and security breaches due to the unconstrained expansion of IoT devices, apps, and platforms. To handle unique access and permission challenges in the IoT, there isn't a universal system in place, though. A secure authorization process protects against unauthorized access requests while ensuring that only authorized entities data and resources can be accessed by (people, machines, etc.). IoT's main issues center on the isolation and security of data and facts. Creating safe connection control and authorization processes is one method for privacy and security addressing challenges in the IOT. Admittance control models for the IOT can now be created using the most well-known portrait in the field, such as Protagonist-based Connection Control (PBCC) [6, 7] and Competency-Based Connection Control (ComBCC) [8]. In recent years, scholars have become more interested in aspect-based connection control (ABCC), an elastic connection control method that assigns rights based on the properties of subjects and objects. Regardless of the advancement of several connection control models for IoT, no formal connection control model or universal authorization technique for stem-based IoT has gained widespread acceptance. It is particularly difficult to build a uniform or standard access control/authorization strategy because there are so many different companies operating in the IoT market[9].

The authorization of present state systems and talk about several crucial security concerns and mistakes in design pertaining to cloud enabled IoT devices have exhibited here. The specific challenges that the Cloud-IoT platform has in providing complete access control and authorization security[10]. One of the main difficulties in preventing unauthorized access to IoT data and devices is developing a elastic and delectable connection control paradigm. An Aspect-Based Connection Control (ABCC) paradigm is provided to safeguard Cloud-Based IoT architecture in order to address this issue. The criteria for connection control and endorsement in these two IOT concerns—a canny house and a canny parking system—are defined in two Cloud-Based IoT use cases that are included. The use cases are explained from a PBAC viewpoint and define qualities for its materials to emphasize the PBAC model's relevance in cloud-enabled IoT. Several devices, such as a light sensor and a smart bulb, may be found in a smart home. The users of the house and these gadgets could share a predetermined set of attributes that indicate the authorizations for each of these entities. Next section goes into great length about the use case analysis and description.

The essay is standardized for the forthcoming portions. In Section II, A succinct overview of the architectures for the cloud, mobile, and IoT are given. In Section III, focused on some of the common connection control strategies as well as the ABAC paradigm for cloud enabled IoT. Two other examples of stem enabled IoT use cases are a canny house and a canny parking setup. IoT data security issues and potential future developments and the study's result is presented in upcoming sections.

2. BACKGROUND OF THE STUDY

This section provides some pertinent backdrop information on IoT and cloud/mobile cloud computing infrastructures.

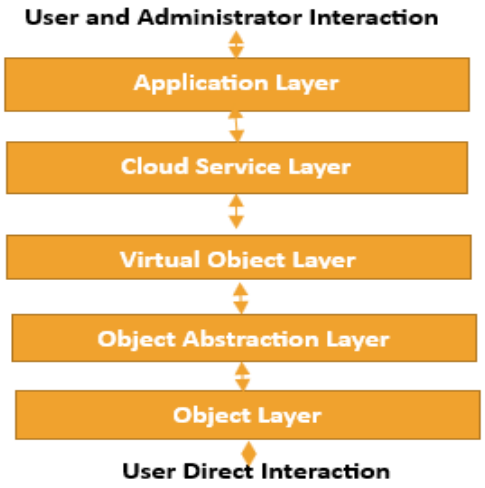

Figure 1. ACO Architecture

The development of machine-to-machine communication, wireless technologies, microcontrollers, and microelectronic mechanical systems contributed to the establishment of the Internet of Things (MEMS). Another element that will encourage the development of the IoT is IPv6, which provides a large Internet addressing space [11]. Billions of intelligent objects in the virtual world can now be individually identified as IPv6 developments. IoT is always changing because "everything" is now associated with the Internet. Because IoT devices[12,13] are also growing smarter because to high tech like stem computing, mobile computing, artificial intelligence (AI), big data analytics, and machine learning. New efficient architectures have been proposed in addition to the conventional cloud computing literature-based models that have been investigated to enrich the enactment of environment on cloud/mobile. In [14], There is a list of simulation tools used to replicate cloud and mobile cloud systems, and each tool's merits and demerits are explored. [15] evaluated the approaches and developments in both general cloud computing and mobile cloud computing.

The high cost of setting up cloud environments is a significant barrier to cloud computing research. The advancement of wireless technologies, micro-controllers, and other components donated to the formation of the IOT. In [16], the advantages and disadvantages of each simulation tool used to model cloud and mobile cloud settings are highlighted. There is a list of simulation tools used to replicate cloud and mobile cloud systems, and each tool's merits and demerits are explored. [17, 18]. Additionally, [19] data security during transmission was emphasized as a crucial problem, particularly when using wireless mobile networks. Some studies suggested employing reliable cryptographic methods on hardware to supply the need. Machine learning and deep learning algorithms have been used for disease diagnosis and sentiment analysis [20-22]. Design, code generation and simulation of IoT environments with mobility devices by using model-driven development and an Edge-Cloud based Reference Architecture to support cognitive solutions in Process Industry [23-25].

A standard IoT architecture typically has three layers: Devices and physical objects are located in the device or perception layer, which is followed by one or more middleware layers, the application overlap, which is the top layer. Actual Internet of Things (IoT) items that users can interact with directly are included in the Object layer. These gadgets gather information from people and their local environment and transmit it to the higher layers of the architecture. The Object Substance layer makes a distinction interpolated the numerous genuine objects and the essential replicas that go along with them. This overlap serves as the cardinal connection control point for real-world by offering a privacy and authorization juncture interpolated the object overlap and further EACO tiers, Internet of Things devices. In contrast to genuine Internet of Things hardware, such as sensors and actuators, it is made up of gateway devices, which have more processing and storage power. Being the this overlap deed as the cardinal connection control mark for actual Internet of Things devices and acts as a privacy and permissions juncture interpolated the object layer and later EACO levels. Instead of sensors and actuators seen in real Internet of Things hardware, it consists of gateway devices with increased processing and storage capacity. The Object Abstraction layer separates the numerous actual items from their corresponding virtual counterparts. By offering an endorsement and isolation juncture interface between the object layer and other EACO levels, this overlap deed as the initial connection control point for Internet of Things devices in the real world. In contrast to genuine Internet of Things hardware, such as sensors and actuators, it is made up of gateway devices, which have more processing and storage power. The Virtual Object layer is made up of computer-generated essential substances that are representations of actual objects.

The summary of this research paper includes Introduction about mobile and cloud computing with security concepts included in section I. Background information about the research work have been included here in the section II. This section focused more on the information on IoT and cloud/mobile cloud computing infrastructures. The role of PBAC(Policy-Based Access Control) in cloud enabled IoT is included and there are two use cases are included under the control models of entry for IoT here in the section III. Section IV involves IoT cloud context authorizations and future directions. Finally, Section V focused on the conclusion part of this paper.

3. PBAC IN CLOUD-ENABLED IOT

In this section, first, review somehow the recently released active connection control techniques for the Internet of Things. The requirements for connection control and permissions considering two Stem-Enabled IoT use scenarios are then analyzed. Also shown how attribute-based access control may be used to secure the Stem-Enabled IoT architecture and meet connection control needs.

3.1. Control Models of Entree for IoT

The RBAC approach, which establishes rights (declares, learn, draft, sign up, etc.) based on pre-defined acts that may be allocated to various substances, such as users and IoT machinery, is currently being used by steam-enabled IoT platforms. Nevertheless, the act-based approach cannot, away, handle the changing needs of cloud-based IoT. Crucial steam-Based IoT platforms used today include special role-based authorization mechanisms that combine access control rules with cryptographic keys and certificates (such X.509 certificates), which are then connected to particular IoT units or things. With the Amazon IoT staging, a true steam-based IoT planning, a formal access control mechanism has been created. This model, referred to as AWS-IoTAC, was developed by expanding the Amazon Cloud Access Control (AWSAC) concept. To provide the AWS-IoTAC miniature extra precise connection control morality such IoT, the authors have suggested a variety of attribute-based access control PABAC) upgrades.

In addition, several academic academics have created numerous other access control models. The authors of a thorough study have offered a thorough reasoning of various IoT connection control mechanisms. The main pillars of IoT access control models are ComBAC models and aspect-based access control (RBAC). An RBAC miniature for IoT has been presented in contrast to Sun et al model which combines RBAC and PBAC(Policy-Based Access Control). This paradigm gives roles to users according to their characteristics rather than determining the authorizations of users on objects. Similar to this, some other hybrid models pair RBAC and PBAC with groups and group attributes.

3.2. Use Cases

3.2.1. A Canny House Use Case

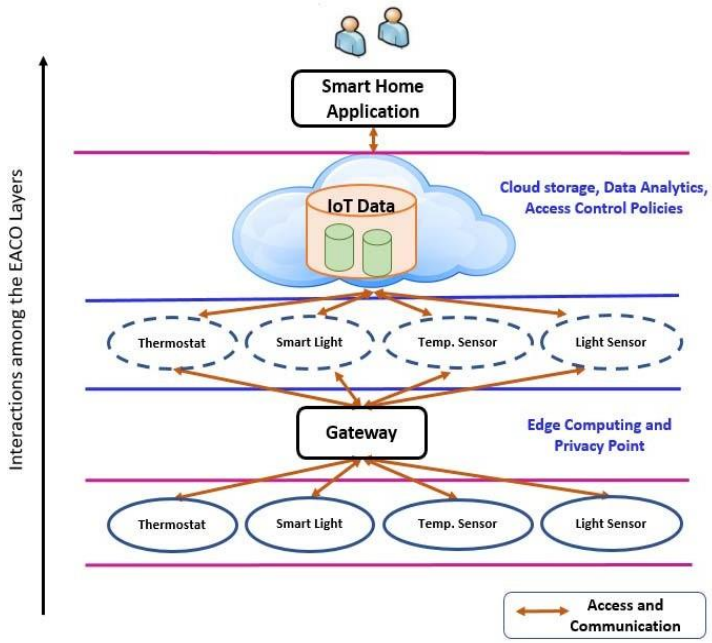

Figure 2. Smart House in EACO

Figure 2 the EACO architecture [26] has a use case in a smart home. A separate element of the use case is represented by each tier of architecture. An example of a physical device found in the object layer is a thermostat. Other examples include a canny lamp, a sensor light, and a sensor for temperature. A portal that validates the devices and facilitates contact with other architectural levels is part of the object abstraction layer. It provides edge computing capabilities and acts as the device and data's access control and privacy point. Each item's (IoT device's) virtual objects are kept in the layer of virtual objects, displayed as dotted circles. The Cloud services layer, where the data is stored, hosts both the authorization guidelines and the data analytics. In order to provide customers with intelligent analysis and forecasts, IoT applications show users the data that IoT devices have collected. The connections and accessibility between these tiers are shown by the arrows. To function, these IoT devices must be securely connected to one another. An attacker can get access to the IoT network by exploiting a device with weak security or one with weak access control and authorization procedures, given the number of physical devices and gateways. A flexible approach to access control is required in cloud-enabled IoT architecture to protect the bond and isolation of people, IoT devices, and assets.

The PBAC technique can be applied to authorized security with use case, where certain authorizations on various entities are either accepted or rejected based on the qualities where various entities are given attributes. An aspect is a brand and cost, where the brand is the name of the characteristic and the cost is inside the attribute's acceptable range of values. The user's age and the device's or user's location are two simple examples of attributes in general. In ABAC(attribute-based access control), each IoT app, service, and device has an identifiable collection of attributes with precise values. Many different values can be included in these attributes, such as strings for location and digits for age. The authorization can then be granted based on these criteria for a variety of people further material. For instance, if a user requests access to a device, both the person's characteristics and the device's attributes must adhere to the established authorization policy in order to grant connection to the device. If the person asking for access to a gadget is its owner and present at home, for example, the policy may grant this person access to the device in order for them to perform an operation, such as turning it on or off. For each permission in ABAC, a specific access control policy must normally be created. If the predicate logic statements in these authorization policies are evaluated as true, the access will be allowed; otherwise, it will be denied. In a similar manner, devices can request to send or receive messages from other devices.

A graded contact between properties could further occur, depending on the usage. In a canny house, similar values would be assigned to the Owner, Spouse, Child, and Guest users based on our roles and locations. An administrator will frequently specify the attributes and their potential values in addition to offering a collection of aspect-based connection control rules such employ customer also device data. In a fictitious smart house, either the owner or the owner's spouse would serve as the administrator who sets policy. While making access control decisions, a variety of contextual elements may be taken into account in addition to user and device data. Consents based on ABAC for multiple users on the entities on the characteristics, as opposed to other access control models like RBAC or CapBAC. For the potent Cloud-Based IoT architecture, this offers elastic assess control and a fine-grained endorsement system based on ABAC endorsement proposition.

3.2.2. A Canny Parking System

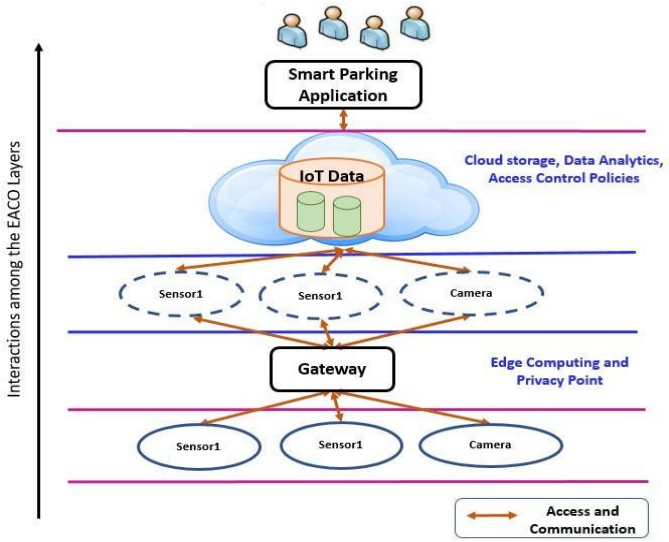

Figure 3. Canny Parking System

Next, go over another cloud based IOT use case, this time a canny parking system that is modified against, point a network of IOT sensors collects data about embracing availability and sends it to the steam. The steam facilities give information to users via applications, such as a smartphone application, after data processing and data analytics. Users can learn about the locations open in various parking lots after being alerted if parking is available. This efficient parking system eventually saves the time that university users, including faculty, staff, and students, would otherwise expend seeking for parking spots.

Figure 3 illustrates a clever EACO(Enhanced Access Control Oriented) - based parking system for universities. The object layer contains sensors (Sensor1 and Sensor2) as well as a camera. To keep an eye on a lot of automobiles and parking spaces, there would be a tony of sensors and cameras in the actual world. The sensors would assemble report on the number of embracing spaces that were available while the cameras would track the volume of traffic in the embracing lots. Computing and analytics are done in the cloud to provide clients with helpful observation and divining analytics on peak parking hours. The gateway and virtual objects transfer the data there. Users can choose preferences for the necessary data when using IoT applications to obtain the data [26].

The information about the parking spaces will vary depending on the user roles, which in this use case include student, faculty, staff, and visitor, as there are specific parking spaces exclusively for students or solely for professors. Additionally, ABAC permission policies change concurrently. For instance, a visitor shouldn't be permitted to park in a faculty member's designated parking space. These use cases demonstrate how a description-based connection control and endorsement system may be deployed successfully using cloud-enabled IoT architecture. The potential ABAC use cases in cloud based IoT platforms are analyzed and proposed in this work. The Amazon Cloud-IoT platform to successfully implement these use cases. By developing complex case entrails and decisive their description and ABAC endorsement needs, we'll further our study into tangible prototypes.

The summary of this part is about the role of PBAC (Policy-Based Access Control) in cloud enabled IoT is included and there are two use cases are included under the control models of entry for IoT here in the section. The first use case for Smart House in EACO (Enhanced Access Control Oriented) and then the second use case is purely for parking system. There have been sensors and cameras used in the multiple layers of the system for monitoring the system.

4. ANALYSIS OF SECURITY IN THE CLOUD-CASED IoT

This article discussed IoT cloud context authorizations that involve users, intelligent IoT devices, Cloud services, and apps. Nevertheless, these IoT devices constantly generate and share massive volumes of data. In many IoT domains, data security and privacy are important considerations. Let consider and example, in a canny healthcare use case where user evidence and report are very sensitive to isolation, the cloud-based IoT architecture increment severe questions about data preservation and retirement. In this arrangement, data from particular devices, data obtained from other sources, and metadata pertaining to IoT items are all stored in the database. various types of data for analysis and predicting the future and diseases. Refuge of Data, Rights of Data, and data isolation and distribution, which are all covered here, are the three key IoT data security and privacy problems.

- **Refuge of Data:** Securing users including device facts is essential in the IOT architecture with cloud. It is necessary to create data access control models for protecting both static data that is kept at various locations, physical hardware, gateways, the cloud, and data that is travelling between various components of the architecture are all examples of architecture.
- **Rights of Data:** Another crucial IoT attitude data with ownership. Identity of Owner of the data like users, devices, cloud assistance providers, or software for the Internet of Things in edict to solve the issue of data ownership, it is vital to recognize the various IoT data sources and consumers and to explain the relationship between IoT entities and data.
- **Data Privacy and Sharing:** Sensors and wearable devices, among other physical items, are sources of IoT data. Then, this data is dispersed over a comprehensive range of organizations, containing hardware, gateways, besides different Cloud services. Data privacy must be addressed if the IOT is to thrive in every expanding linked world.
-

Possible directions in privacy and security in data with IOT for future research directions in Cloud architecture.

5. CONCLUSION

The authorization processes for two Cloud-Enabled IoT use cases in this study have exhibited, demonstrating how ABAC offers a flexible and safe authorization method for Cloud-Enabled IoT architecture. Although different policies are applied to the access of people, resources, and devices,

contemporary authorization strategies concentrate on an act-based or behavior-based approach. Once created and precise to certain organizations, these jobs and policies can be challenging to manage and may result in a proliferation of roles and policies, creating the issue of act-explosion and behavior-explosion. ABAC is a method that may be able to manage the needs for admittance control and endorsement in a potent Cloud-Enabled IoT scenario. In the upcoming work, it is projected to investigate the potential future avenues and integrate our use cases into a natural-world Cloud-IoT platform to establish data admittance control and endorsement models. Consequently, models that take security concerns into account in the future could be created without sacrificing system advantages or the time and energy limits of mobile users. To ensure minimum overhead, models can also be created.

REFERENCES

[1] Lo'ai, A. Tawalbeh, and Waseem Bakhader(2016). A Mobile Cloud System for Different Useful Applications. In 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 295-298. IEEE.

[2] Bhatt, Smriti, Farhan Patwa, and Ravi Sandhu(2017). An Access Control Framework for Cloud-Enabled Wearable Internet of Things. In 3rd IEEE International Conference on Collaboration and Internet Computing (CIC), 2017. pp. 328-338. IEEE.

[3] Chandan, Radha Raman, Awatef Balobaid, Naga Lakshmi Sowjanya Cherukupalli, Gururaj H L, Francesco Flammini, and Rajesh Natarajan. 2023. "Secure Modern Wireless Communication Network Based on Blockchain Technology" Electronics 12, no. 5: 1095.

[4] Ferraiolo, David F., Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli (2001). Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security (TISSEC) 4. no. 3: 224- 274.

[5] Hernández-Ramos, José L., Antonio J. Jara, Leandro Marin, and Antonio F. Skarmeta (2013). Distributed Capability-Based Access Control for the Internet of Things. Journal of Internet Services and Information Security (JISIS) 3.1-16.

[6] Jin, Xin, Ram Krishnan, and Ravi Sandhu (2012). A Unified Attribute- Based Access Control Model Covering DAC, MAC and RBAC. In IFIP Annual Conference on Data and Applications Security and Privacy. pp. 41-55. Springer, Berlin, Heidelberg.

[7] Hu, Vincent C., David Ferraiolo, Rick Kuhn, Arthur R. Friedman, Alan J. Lang, Margaret M. Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone (2013). Guide to Attribute Based Access Control (ABAC) Definition and Considerations (draft). NIST Special Publication800, no. 162.

[8] Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. 2023. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0" Infrastructures 8, no. 2: 22.

[9] Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent From 2015(2017). https://www.gartner.com/newsroom/id/3165317.

[10] Tawalbeh, Lo'ai, Norah Alassaf, Waseem Bakheder, and Alaa Tawalbeh(2015). Resilience mobile cloud computing: features, applications and challenges." In 2015 Fifth International Conference on e-Learning (econf), pp. 280-284. IEEE.

[11] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu(2013). Mobile Cloud Computing: A Survey. Future Generation Computer Systems 29, no. 1, 84-106.

[12] Bahwaireth, Khadijah, Elhadj Benkhelifa, Yaser Jararweh, and Mohammad A. Tawalbeh(2016). Experimental Comparison of Simulation Tools for Efficient Cloud and Mobile Cloud Computing Applications. EURASIP Journal on Information Security 2016, no. 1,15.

[13] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis(2012). Fog computing: Mitigating insider data theft attacks in the cloud. In 2012 IEEE symposium on security and privacy workshops, pp. 125-128. IEEE.

[14] Tawalbeh, Lo'ai A., Fadi Ababneh, Yaser Jararweh, and Fahd AlDosari(2017). Trust delegation-based secure mobile cloud computing framework. International Journal of Information and Computer Security 9, no. 1-2, 36-48.

[15] Prabhdeep Singh, & Ashish Kumar Pandey. (2022). A Review on Cloud Data Security Challenges and existing Countermeasures in Cloud Computing. International Journal of Data Informatics and Intelligent Computing, 1(2), 23–33. https://doi.org/10.5281/zenodo.7464700

[16] Ragini., Mehrotra, P., Venkatesan, S(2014): An Efficient Model for Privacy and Security in Mobile Cloud Computing. International Conference on Recent Trends in Information Technology, 1-6.

[17] Liu, Y., Lee, M.J(2015).: Security-Aware Resource Allocation for Mobile Cloud Computing Systems. Computer Communication and Networks (ICCCN), 24th International Conference on, 1-8.

[18] Liang, H., Huang, D., Cai, L.X., Shen, X., Peng, D(2011).: Resource Allocation for Security Services in Mobile Cloud Computing. IEEE INFOCOM 2011 Workshop on M2MCN, 191-195.

[19] Manju Bargavi, M.Senbagavalli, Tejashwini.K.R, & Tejashvar.K.R. (2022). Data Breach – Its Effects on Industry. International Journal of Data Informatics and Intelligent Computing, 1(2), 51–57. https://doi.org/10.5281/zenodo.7469630

[20] M, Senbagavalli., G T Arasu(2016): Opinion Mining for Cardiovascular Disease using Decision Tree based Feature Selection. Opinion Mining for Cardiovascular Disease using Decision Tree based Feature Selection, volume 6,issue 8, 891-897.

[21] Valli, M S., G, T, Arasu(2016): An Efficient Feature Selection Technique of Unsupervised Learning Approach for Analyzing Web Opinions. Journal of Science and Industrial Research, NIScPR Online Periodicals Repository, 221-224.
[22] M. Senbagavalli, V. Sathiyamoorthi, S.K. ManjuBargavi, Swetha Shekarappa G., T. Jesudas(2023): Deep learning model for flood estimate and relief management system using hybrid algorithm. Artificial Intelligence and Machine Learning in Smart City Planning. Pages 29-44.
[23] José A. Barriga, Pedro J. Clemente, Miguel A. Pérez-Toledano, Elena Jurado-Málaga, Juan Hernández(2023). Design, code generation and simulation of IoT environments with mobility devices by using model-driven development: Simulate IoT-Mobile. Pervasive and Mobile Computing Volume 89.
[24] Belen Bermejo, Carlos Juiz (2023): Improving cloud/edge sustainability through artificial intelligence: A systematic review. Journal of Parallel and Distributed Computing. Volume 176, Pages 41-54
[25] Antonio Salis, Angelo Marguglio, Gabriele De Luca, Silvia Razzetti, Walter Quadrini, Sergio Gusmeroli(2023): An Edge-Cloud based Reference Architecture to support cognitive solutions in Process Industry. Procedia Computer Science Volume 217, Pages 20-30.
[26] Smriti Bhatt, Lo'ai A. Tawalbeh, Pankaj Chhetri, Paras Bhatt(2019): Authorizations in Cloud-Based Internet of Things: Current Trends and Use Cases. in Fourth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE.

BIOGRAPHIES OF AUTHORS

M.Anitha is working as an Assistant Professor in the Department of Computer Science and Engineering, Kingston Engineering College, Vellore, TamilNadu. She completed her Bachelor of Engineering from Bharathidasan University in Thichy, Tamil Nadu. She has completed her Master of Engineering in Computer Science and Engineering from Anna University, Chennai, Tamil Nadu. She has pursuing Doctorate from Anna University, Chennai. She has nearly two decades of experience in the field of Teaching. She is an active member of the IAENG. Her Specialization includes Artificial Intelligence, Data Science and Analytics. She delivered guest lectures to various colleges. She has published many chapters and papers in national and international conferences and journals. She can be contacted at email: anitham.apcse@gmail.com

M.Senbagavalli is working as an Associate Professor in the Department of Computer Science & Information Technology, Alliance College of Engineering and Design at Alliance University, Bangalore. She completed her Bachelor of Engineering from Periyar University in Salem, Tamil Nadu. She has completed her Master of Engineering in Computer Science and Engineering from Anna University, Chennai, Tamil Nadu. She also completed her doctorate in computer science and engineering from Anna University in Chennai, Tamil Nadu. She has nearly two decades of experience in the field of Teaching. She is an active member of the Institute of Green Engineers, IET and lifetime member of Institute of Researchers, APR, IAENG and the Society of Professional Engineers, Malaysia. Her Specialization includes Artificial Intelligence, Data Science and Analytics. She is the treasurer in the Rotary Club of Global Scholars. She delivered guest lectures to various colleges on recent technologies, and she acted as panel member for the Tech conference in different colleges. She received many national and international awards from reputable organizations. She has filed and published Indian and Foreign patents. She has published many chapters and papers in national and international conferences and journals. She is the reviewer of many international and national journals, namely IEEE, Springer, and Elsevier. She can be contacted at email: senba1983@gmail.com