Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P.6939-6948 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

IoT Collected Health Data to Store in Cloud and Access with PCMAE

M.Reena Ivanglin, Dr. R.Pragaladan

[1.] PhD Research Scholar, Department of Computer Science, Sri Vasavi College, Erode.
[2.] Associate Professor & Head Department of Computer Science, Sri Vasavi College, Erode.

How to cite this article: M.Reena Ivanglin, R.Pragaladan (2024) Cybersecurity IoT Collected Health Data to Store in Cloud and Access with PCMAE. *Library Progress International,* 44(3), 6939-6948.

ABSTRACT

Cloud storage is a utility where data is remotely stored cloud environment and then the data is accessible to end users over internet. It permits the client to collect the files through online and access from anywhere via internet. The main objective of the cloud storage is to store the data safely in the Cloud space and fetch the data whenever requested by the client. In this research analysis the IoT devices collected data (IoT-PCM) are store into the cloud and access the data from the cloud. Here we are used the private cloud (AWS) for data storage purpose and the IoT devices collects the patient health data. In proposed PCMAE (Patient Care Monitoring based Authorized Encryption) technique it provides a secured way to view the health data, decrypting with verified secret key before downloading. Main work on how the doctors retrieval the IoT- PCM health data.

Keywords: Private cloud, cloud storage, cloud security, encrypting, decrypting.

1. Introduction

Cloud refers to the network that provides services to network through internet. It is a model that enables the characteristics like on demand self-service, pay-as-you-use-service.[1] Cloud specialist co-ops are planned to give various capacity services. Clients will be profited as they can store substantial measure of information in outsider stockpiling sparing their very own framework space. The most essential and noticeable issue to be tended to is security. Cloud server providers offer different security components, however ifenemy gains admittance to the client's information; at that point it influences the protection of the client. Security ought to be accommodated touchy information of the client through different authentication and approval components. For the most part client information is verified by encryption and unscrambling techniques. [2] This avoids the cost of building and maintaining their data store. But the users need to provide privacy for the data and to be able to search it without losing privacy. The users always search their documents through keyword in plaintext, which may leak privacy of users in cloud storage environment. To keep user data confidential against an untrusted cloud, a natural way is to apply cryptographic approaches, by disclosing the data decryption key only to authorized clients. [3] The proposed model has been structured by bringing together various techniques and utilizing them to perform the task of data security in cloud. Apart from this, the model positively handles the security issues by employing strict authentication techniques, like login-id and password. Thus all about the techniques result into a defined mechanism that encourages the proper functioning of cloud computing. In this computing model, owner sends the encrypted data to cloud where it is stored in different sections depending on the sensitivity rating and then the data can be retrieved by user from the cloud when requested. However, this is achievable only after passing the authentication techniques. [4]

2. Related Works

S.Kalaivani, A. Senthil Kumar et.al[5] Cloud computing is fast growing technology that enable the users to store and access their data remotely. Using cloud services user can enjoy the profit of on-demand cloud applications and data with limited local infrastructure accessible with them. Research is going on to provide secure data sharing with enhanced user privacy and data access security. The proposed model of ABAC addresses the security features for data access, privacy preserving and secure sharing of data in cloud environment and use the hybrid cloud storage architecture that allow the users to store their bulky data securely in a public cloud and store the sensitive information related to data access on private cloud. In this technique the privacy is managed by the owner of the data itself and the secure sharing of data is provided. It is believed that the proposed model has the potential to be helpful in commercial situations as it uses the practical access policies in the cloud environment.

Yahia Alemami, Ali M. Al-Ghonmeinet.al[6]describes a set of encryption algorithms (advance encryption standard (AES), data encryption standard (DES), Blowfish, Rivest-Shamir-Adleman (RSA) encryption, and international data encryption algorithm (IDEA) was compared in terms of security, data encipherment capacity, memory usage, and encipherment time to determine the optimal algorithm for securing cloud information from hackers. Results show that RSA and IDEA are less secure than AES, Blowfish, and DES). The AES algorithm encrypts a huge amount of data, takes the least encipherment time, and is faster than other algorithms, and the Blowfish algorithm requires the least amount of memory space. RSA and IDEA are less secure than AES, Blowfish, and DES, and the Blowfish algorithm requires the least amount of memory space. The AES algorithm can be used for encrypting huge amounts of data. The AES is faster than other algorithms and is the best algorithm in terms of authentication parameters. The RSA consumes the most memory and requires maximum execution time.

Waleed T. Al-Sit, Hani Al-Zoubiet.al [7] aimed to review these techniques with their security challenges by presenting the most popular cloud techniques and applications. Homomorphic Encryption method in cloud computing is presented in this paper as a solution to increase the security of the data. By using this method, a client can perform an operation on encrypted data without being decrypted which is the same result as the computation applied to decrypted data. The approach of Homomorphic Encryption in cloud computing is presented and most security challenges at different levels of cloud computing with applications of vulnerabilities are explained. In addition, the most popular methods used to achieve the required level of security are presented as well. Cloud computing provides many facilities, flexibility, availability, but it faces security issues, so stringent security enforcement should be applied to ensure that the IT environments are more secure.

Ming Li, Shucheng Yu et.al[8] In this literature, using online Personal Health Record (PHR) as a case study, we first show the necessity of search capability authorization that reduces the privacy exposure resulting from the search results, and establish a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data. Andthen propose two novel solutions for APKS based on a recent cryptographic primitive, Hierarchical Predicate Encryption (HPE). The solutions of enable efficient multi-dimensional keyword searches with range query, allow delegation and revocation of search capabilities. Moreover, to enhance the query privacy which hides users' query keywords against the server. To propose a scalable, fine-grained authorization framework where users obtain their search capabilities from local trusted authorities according to their attributes. And then propose two novel solutions for APKS over encrypted data based on HPE, where in the first one we enhance the search efficiency using attribute hierarchy, and in the second we enhance the query privacy via the help of proxy servers.

Muhammad Bilal Qureshi, Muhammad Shuaib Qureshi et.al [9]the main objective of the cloud computing system is to provide on-demand storage and computing resources to the users on the pay-per-use policy. It allows small businesses to use top-notch infrastructure at low expense.The Blowfish algorithm stands out amongst symmetric encryption algorithms. When there is a limitation on processing power and time, the AES is the most secure of the symmetric algorithms. The RSA algorithm is an asymmetric algorithm that is suitable where confidential information is to be shared because its public-private key pair security is more ensured. Currently, ongoing research is finding an encryption algorithm that scales well with increasing data generated with high speed by

smart systems and is efficient in performance. Data security is the main hindrance due to which smart systems management is hesitant to shift their data to the cloud. Keys used for data encryption and decryption should be more secured so that a third party cannot hack authentication details.

Fakher Abbas et.al [10] thisliterature provides an in-depth exploration of data encryption techniques used in the cloud, including symmetric encryption, asymmetric encryption, and homomorphic encryption. Additionally, the literature examines key management strategies to effectively safeguard encryption keys and maintain secure data access. By understanding the various encryption techniques and implementing robust key management practices, organizations can fortify their data protection efforts in the cloud, mitigating the risks associated with data breaches and unauthorized data access. Balancing data security with encryption performance and integrating encryption into cloud services are critical for end-to-end data protection. As cloud computing continues to evolve, addressing key challenges and exploring emerging encryption trends will be essential to maintaining a secure and resilient cloud computing environment.

Yamuna, B.Moshe (11) proposed efficient secure data retrieval is developed with the help of multi-stage authentication(MSA) and optimized blowfsh algorithm (OBA). To increase the security of the system, the keyvalue is optimally selected with the help of a binary crow search algorithmThis will avoid, un-authorized person toattack the data.

Kanna and Vasudevan (12) had developeda hybrid crypto mechanism-based privacypreservation on the cloud. The cryptomechanism was designed based on a fullyhomomorphic–elliptic curve cryptography(FH-ECC) algorithm. Afterencryption process data was stored on thecloud. After the storage process, the accesscontrol policy was developed to avoid theunauthorized person login.

3. Data Storage framework for the Cloud

Cloud Storage uses remote servers to save the patients health data which are collected by IoT devices. Users upload data to servers via an internet connection, where it is saved on a virtual machine on a physical server. To maintain availability and provide redundancy, cloud providers will often spread data to multiple virtual machines in data centers located across the world. If storage needs increase, the cloud provider will spin up more virtual machines to handle the load. The patient health data contains the patient's temperature, pulse, and circulatory strain whenever the specialist or well-being focus requests information about the patient's health. Before the scramble and key age processes are carried out, it is not difficult to store these subtleties in that state of mind. The information gathered is safely stored in the private AWS Cloud. But when data stores into the cloud there is some security needs. For this purpose we need some security technique of preserving data confidentiality by transforming it into cipher text, which can only be decoded using a unique decryption key produced at the time of the encryption or prior to it to store data in the cloud like encryption and decryption.The cloud user strives to just save plain text data (pt) in an encrypted message that use the Ascon private keys (pk). The Ascon is probably more suited to making sure data transfer and storage security. Invaders who have not had right to possession are still unable to access this same plain data. Unauthorized access cloud users have already had access to data on occasion.

*Data Collection Process:*The IoT equipment is associated with patient body. The gadget additionally interfaces the organization like Bluetooth to versatile or Wifi to the organization straightforwardly. Then, at that point, its gather the information and shipped off the worry client. The body sensor measures the patient's temperature, pulse, and circulatory strain whenever the specialist or well-being focus requests information about the patient's health. These data are called IoT – PCM (Patient Care Monitoring). These data are needed to store securely into the cloud.

*Data Storage using encryption process:*IoT-PCM data are needed to store into the cloud. The IoT-PCM now in a plain text (readable) format so, need to provide more security. For this purpose the Encryption is one of the most widely used and successful data protection technologies in today’s corporate world. Using this technique plain text converted into cipher text (ct) (unreadable) format. Data encryption converts data into a different form (code) that can only be accessed by people who have a secret key (formally known as a decryption key) or password.

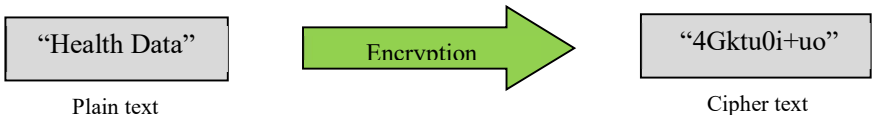
The code key created by this network is utilized in the Ascon Lightweight Authenticated Encryption technique.

Ascon Lightweight Authenticated Encryption: It is an approved encryption and hashing (fixed or variable outcome length) with a lone lightweight change. Lightweight crypto is symmetric encryption technology that works well on forced frameworks, like the Internet of Things (IoT), because chips with limited capacities are used.

States of Data Encryption: Data, whether it's being transferred between users or stored on a server, is valuable and must be always protected.

Data encryption in transit: Information that is actively travelling from one point to another, such as via the internet or over a private network, is referred to as data in transit.

Encryption of data at rest: Data at rest refers to information that is not actively moving from one device to private cloud in another way. Due to device security features restricting access, data at rest is often less vulnerable than data in transit, but it is still vulnerable.



Encryption is used to prove the integrity and authenticity of the information. Here we are implementing the ASCON lightweight encryption technique which leads to encrypt the patients' health data collected by IoT devices.

4. Public Cloud Vs Private Cloud

Public clouds are the most common type of cloud computing deployment. The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the internet. With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments. With the public cloud, third-party service providers manage on-demand computing infrastructure and deliver them to multiple companies over the Internet.
Private clouds sometimes referred to as a data center reside on a company's own infrastructure, typically firewall protected and physically secured. Mature organizations that have heavily invested in on-premises infrastructure frequently leverage that investment to create their private cloud. Compared to Public Cloud, a multi-tenant cloud environment where resources are shared among multiple users, AWS Private Cloud provides dedicated resources for a single user or establishment. This allows for greater control over the infrastructure and data and improved security and compliance. While Public Cloud offers on-demand scalability and cost-effectiveness, AWS Private Cloud provides a higher level of customization and control, making it a good choice for organizations with particular compliance concerns or high-security demands.
Private Cloud is also a good option for corporations that require the use of legacy applications or have hardware requirements.Data security and compliance are paramount in healthcare, and AWS excels in this area. It provides robust security features such as encryption, access controls, and threat detection to safeguard sensitive patient information from unauthorized access.

5.Data Access from the cloud storage

In Cloud client can remotely store and bring their information depending on their work need or interest, and cloud is very cheap and dependable too. In proposed technique it provides a secured way to upload the information by encrypting it before being uploaded to cloud and decrypting with verified secret key before downloading. Particularly, to ensure the confidentiality of doctors requests are sensitive data need to be securely downloading from the cloud server. [13]The authentication process is crucial to avoid data loss, data theft, and malicious attack may happen in the data access process also. Especially in a cloud environment, unauthorized clients can easily

transfer data without the data owner's knowledge, meaning that a security breach is inevitable. To avoid this problem, in this journal, PCMAE is proposed to securely access the data on the cloud. The proposed system to handle the tricky encrypted IoT-PCM data sharing with patients in cloud-assisted health data systems, by using patient care monitoring Access mechanism based keyword search, which dramatically alleviates the work intensity of the doctor. The system model is depicted with the private key generator (PKG), cloud server, doctor.

Data Owner: As an original data owner, they could generate and encrypt the patient health data by using the Ascon encryption algorithm. Specifically, the doctor could authorize a trusted assistant by singing an authentication certificate to encrypt the keywords on behalf of him/her, and upload them as well as the encrypted the respective data to the cloud server associated with patient health information systems punctually.

Doctor Registration: In the registration stage, doctors have entered their information on local data base. In primary process of the doctors are needs to register their details to access the respective patient health data in the cloud which may contain the username and password (Uid and pwd). These login details are stored in the local system database. As a data receiver, with the private key, doctor generates a trapdoor corresponded with a specific keyword, and submits it to a cloud server associated with health information systems to retrieve the patient health data in a confidential way.

Cloud server: It provides massive data storage services and has powerful computing capabilities. Particularly, it could run the testing algorithm of PCMAE (Patient Care Monitoring based Authorized Encryption) to enable the authorized encrypted health data sharing, between a patients data in the cloud and doctor.

PKG: It is a fully trusted entity, which is in charge of issuing the private key of any identity, e.g., a doctor, an assistant, or a patient. Also, PKG with a database could support user's inquiry and enable revocation operations in cloud-assisted patient health information systems.

System Initialization: The system initialization is performed by the PrivateKeyGenerator(PKG). Here we are creating the PKG using WG Cipher model.To create private and confidential keys prior to running the capabilities to produce ciphertext and plaintext.

KeyExtract: Taking as inputs the public parameters, the secret key pair, and, the PKG outputs the corresponding private key*pk*of *p and q*.

*Authorized key generation:*Key management emerges as a critical aspect of data encryption, as the security of encrypted data relies on the confidentiality and accessibility of encryption keys as well as decryption keys. We will delve into key management strategies that effectively protect encryption keys from unauthorized access and ensure seamless data access for authorized users. [10] Proper key rotation, secure storage, and access control mechanisms will be discussed to enhance key management practices. This is to generate the authorized private key pair of an assistant, as well as its corresponding authorized parameter like p and q. PKG publishes the corresponding authorized parameter *p and q* and stores the authorized secret request in- formation in its database. To create public and confidential keys prior to running the capabilities to produce ciphertext and plaintext. WG cipher is a simultaneous stream figure that comprises a WG key stream generator. The key stream delivered by the generator is added bitwise to the plaintext to generate the ciphertex(ct).

PCMAE Mechanism: Taking as inputs the parameters *p and q*, the key word *kw*, the authorized private key *pk*, and a data receiver's(doctor) identities*IDr*, the assistant outputs an patient care monitoring based approved ciphertext(ct) associated with *Double Pi algorithm*. Moreover, the secret door techniques available to the private, although the Secret door algorithm in the double Pi algorithm requires the recipient's secret key as insight.

Trapdoor: Taking as inputs the public parameters *p and q*, the private key p*k* of a health data*IDh, receiver IDr*produces a searchable trapdoor *Tkw* corresponded with the keyword, and submits it to the cloud server to retrieve the encrypted health data.

Test: When cloud receives a question from the registered doctors, it utilizes its secret key to pre-process the trapdoor and all double pi cipher texts before having to send some extensive testing to the cloud while trying to conceal the trapdoor and double pi cipher texts. Finally, the cloud server returns the corresponding encrypted IoT-PCM health data to the doctor for data access or retrieval.

Algorithm:

Step 1: Generates the system parameters *p and q* using the security parameter of login details of user id and password as input (doctor).

Step 2: The second step is to generate a key. Returns the public/secret keys (pkFS; skFS) for a cloud based on the set parameters followed based on step 1.

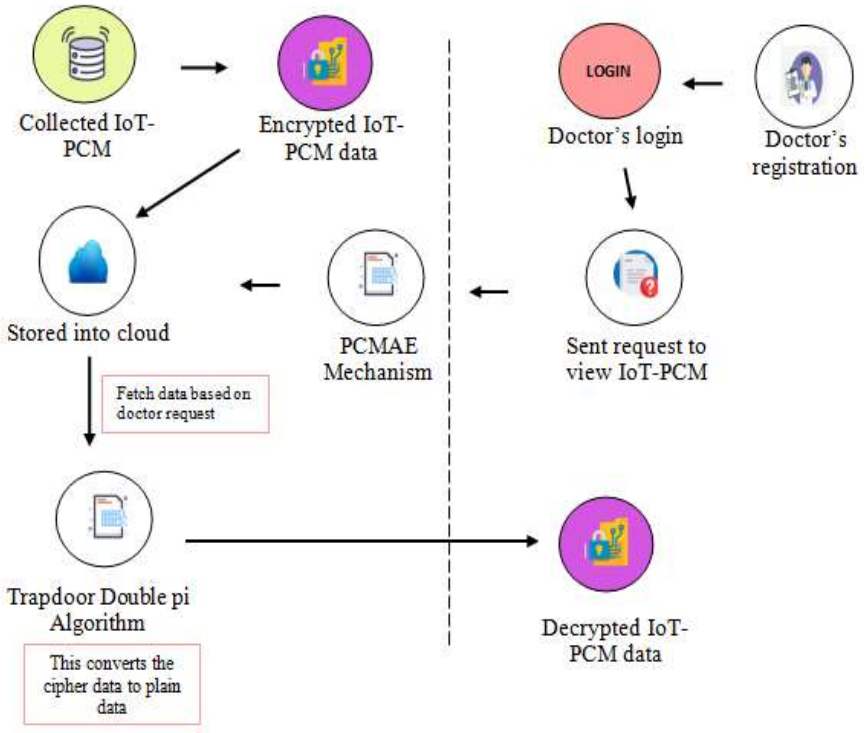


Figure 1: Proposed Architecture of Cloud data Access

Step 3: As per the parameters, it takes front clouds private key pk, which needs to return the Dpi (double Pi) ciphertext.

Step 4: Trapdoor (P and q; pk): Takes parameters, the private key pk of the cloud, the public as inputs and outputs for trapdoor of the health data *IDh* in the cloud.

Step 5: This function that precedes as input parameters the cloud private key pk, a Dpi ciphertext.

Step 6: This step finally the receiver IDr (doctor) receives the IoT based Patient health data *IDh*.

5. Experimental Result

The IoT equipment is associated with patient health data. Body sensors like temperature sensors, blood pressure sensors, and heart rate sensors are fixed to the human body. The respective sensors are collecting patient health data. The collected patient health data is stored in the Cloud information from unauthorized access.

Parameters	Public Cloud	Private Cloud
Infrastructure	Multiple users-shared network managed by service provider	Single user-dedicated network managed by the technical team
Scalability	Easily scalable as per the requirement	Depends on the service provider agreement
Expense	Most affordable cloud that also offers a pay as go services	High investment cost to set up the network and staff with regular
Performance	Multiple users might reduce the performance	High performance for the dedicated users
Security	Less security as the platform is shared	More security as the platform is shared

Table 1 : Comparison of Private and Public Cloud

In the proposed system implementation done in the System using Intel core i3 4th Gen 2.4 GHz Speed Processor with 8 GB and 500 GB Hard Disk. The Collected Patient Dataset is shown below Image.

PatientId	Date	BPH	BPL	HR	TEMP
52820	12-10-2023	110	70	60	97
52822	24-11-2023	140	82	65	97
52700	01-12-2023	140	80	70	98
52818	06-12-2023	110	20	60	96
52840	02-01-2024	130	80	60	96

Parameters	Public Cloud (ms)	Private Cloud (ms)
Data Store Time	16	13
Encryption Time	13	11
Decryption Time	15	12
Data Access	14	11

Table 2: Processing time between the Public cloud and private cloud

The above table describes the difference of the public and private cloud. This table clearly explains the details of the parameters like data store time, encryption time, decryption time, and data access from the cloud respectively.

This system is starts to monitor the parameters of patient's body temperature, heartbeat, blood pressure levels are collected and stored into the Cloud and transmission these data through the wireless body are networks. The IoT based PCM collects and encrypt the health data using ASCON algorithm.

These encrypted data are stored into the private cloud named as AWS cloud. When the doctor sends the request to monitor the IoT based PCM patient data, they must login their details , after that the system verify the Approved key of the doctor, the Trapdoor mechanism based double pi algorithm used for the Key process. If the doctor Key details were does not match means the PCMAE was declined the login process. If the doctor Key match means the PCMAE mechanism to authenticates the key of receiver (doctor). After the successful of login process the doctors view the patient Data.

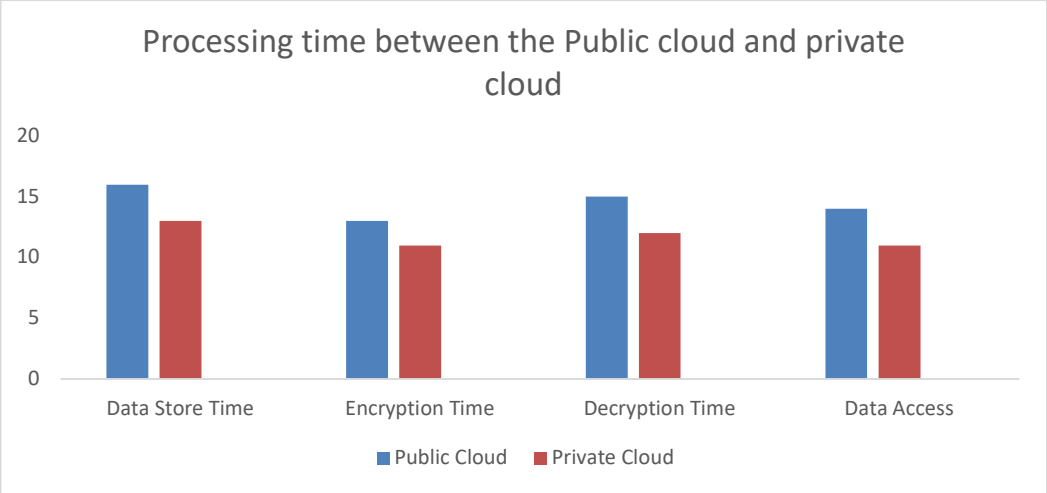


Chart1: Processing time between the Public cloud and private cloud

The following table provide the data of Doctor access the cloud for retrieve patient data. The proposed mechanism efficient work and compare with some parameters. The proposed model compared with the existing model of 11,12 paper . The result will show the following table.

Parameters	FH-ECC Model %	MSA and OBA %	ASCON and PCMAE %
Data Security	80	85	93
Confidentiality	85	89	95
Authentication issue	15	9	5
Availability	88	94	97
Privacy	80	92	98

Table 3: IBE and ASCON – PCMAE

The IBE model provides efficient security and privacy of the patient data, but the ASCON and PCMAE combination provides high efficient safety and availability of the patient health care data. The following chart will show the above table values.

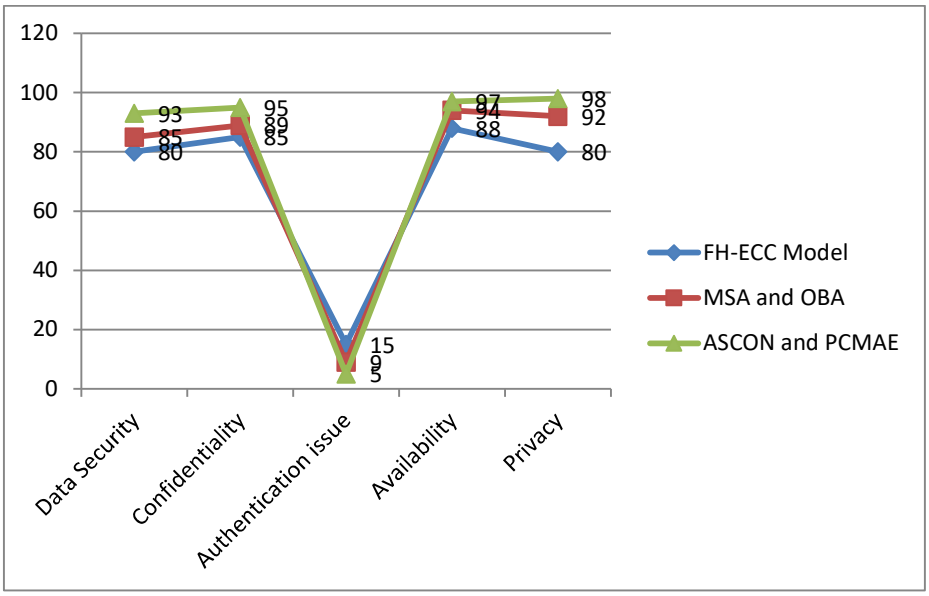


Chart 2: IBE and ASCON – PCMAE

6. Conclusion

In this analysis describes the IoT-PCM data are encrypted and stored into the private cloud. The proposed model was implement the encrypt process of IoT-PCM data using the ASCON algorithm. And the doctors sent request to view the IoT-PCM data. For this purpose the PCMAE mechanism, Trapdoor and the double pi techniques are implemented to view the health data stored in the cloud. The proposed mechanism results have demonstrated that PCMAE is much more practical for the deployment of cloud-assisted IoT-PCMinformation systems for securely retrieve the data.

References

[1] Jeevitha B. K., Thriveni J., "Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey", International Journal of Computer Applications (0975 – 8887), Volume 156 – No 12, December 2016.

[2] K. Ravindranath, M.S. Sandeep Reddy, "Secure Data Storage and Retrieval in the Cloud", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-6S, April 2019.

[3] Anuradha N. M, G. A. Patil, "Secure and Efficient Data Retrieval in Cloud Computing", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS041017 www.ijert.org (This work is licensed under a Creative Commons Attribution 4.0 International License.) Vol. 4 Issue 04, April-2017.

[4] Nagendra Kumar, Ashok Verma, "Access, Identity and Secure Data Storage in Private Cloud using Digital Signature", Vol. 2, Issue 3, March 2018.

[5] S.Kalaivani, A. Senthil Kumar, "Cloud Computing Security Guidance for Encrypted Data Transfer", International Journal of Computer Science and Information Technology Research ISSN 2348-120X, Vol. 5, Issue 3, pp: (15-19), Month: July - September 2017.

[6] Yahia Alemami, Ali M. Al-Ghonmein, "Cloud data security and various cryptographic algorithms", International Journal of Electrical and Computer Engineering (IJECE) Vol. 13, No. 2, April 2023, pp. 1867~1879.

[7] Waleed T. Al-Sit, Hani Al-Zoubi, "Cloud Security based on the Homomorphic Encryption", (IJACSA)

International Journal of Advanced Computer Science and Applications, Vol. 10, No. 8, 2019.

[8] Ming Li, Shucheng Yu, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing", 2020.

[9] Muhammad Bilal Qureshi , Muhammad Shuaib Qureshi, "Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud", 28 March 2022.

[10] Fakher Abbas, "Data Encryption in the Cloud: Techniques and Key Management Strategies", 19 July 2023.

[11]S. YAMUNA , B.MOSHE et all , “Efficient Secure Data Retrieval On Cloud UsingMulti-Tage Authentication And Optimized Blowfish Algorithm” , International Journal of Techno-Engineering, 2023

[12]S. Immaculate Shyla1 · S. S. Sujatha, “Efficient secure data retrieval on cloud using multi-stageauthentication and optimized blowfish algorithm”, Journal of Ambient Intelligence and Humanized Computing, 2021

[13] S. Immaculate Shyla, S. S. Sujatha, "Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm", Journal of Ambient Intelligence and Humanized Computing, 2021.