2022 First International Conference on Artificial Intelligence Trends and Pattern Recognition (ICAITPR) | 978-1-6654-2521-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAITPR51569.2022.9844196

E-Health Security on Could Computing and its Challenges

*A Preethi Vinnarasi**
Research Scholar,
Department of ECE,
SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India
pa9361@srmist.edu.in

R Dayana
Assistant Professor,
Department of ECE,
SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India.
dayanar@srmist.edu.in

P Malarvezhi
Assistant Professor,
Department of ECE,
SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India.
malarvip@srmist.edu.i

K. Vadivukkarasi
Assistant Professor,
Department of ECE,
SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India.
vadivukk@srmist.edu.in

***Abstract*— Healthcare credentials digitized on Cloud has reformed the access of healthcare solutions widely; where patient's medical history is recorded periodically on Cloud and can be accessed based on necessity legally. Cloud services and storage has become a gateway for many services globally with multiple storage providers providing storage facilities to access. This paper enumerates the benefits of Electronic Healthcare on cloud and tribulations based on security and privacy, where the concern is a substance, which itself holds a pack of catalogues such as Confidentiality, Integrity, Data Violation, Reliability, Network eavesdropping, Denial of service, Collusion, etc. The foreground of this paper is a survey with different problems and solution possibilities discussed based on cloud storage and communication on security and privacy issues faced and discussed on work papers which are originally published for Electronics Health Records (EHR) or Electronics Medical Records (EMR). The pros and cons of each approach and results are conferred in this literature survey along with the definitions of cloud computing, its types and existing technologies.**

Keywords*— *E-health, Cloud Computing, Privacy, Security.

I. INTRODUCTION

Cloud Computing is a prevalent word and has become an established genre in the recent decades, storage of information is enfilade where safety and privacy of documents is paramount due to digitization. Records of information and documents are not carried unless it intended to deal with and discuss it, Cloud storage and communication [1], [2] caters solution by storing data in digitized form and provide access to them when in need it which is show in Figure 1.[3], [4].

There are many cloud service providers[5] such as Oracle cloud, Amazon's Amazon web services (AWS), VMware Cloud, Google cloud platform provided by google, Cloud Services by IBM, Microsoft azure, Alibaba Cloud, etc.; they are predominantly overwhelming in providing traditional services and adaptable services based on the new environment for Cloud services.

Electronic Health Records (EHR)[6] or Electronics Medical Records (EMR)[7] or E-Health Records[6], [8]–[12] are data records of Patients with medical history in long term or short term need their medical data if met with new health practitioner or their attender after a long time.

Health practitioners, laboratory testers, and nurses can upload information such as schematics, patient medical information, prescriptions, hospital or clinical reports, radiological photos, billing information, and other sensitive patient information that is kept in the cloud. These data's are observed and recommended based on requirements for security and privacy that follows the Health Insurance Portability and Accountability Act (HIPAA)[12].

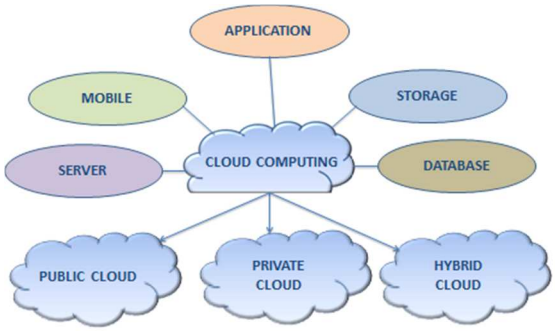

Fig. 1. Cloud Computing

Hospital with Cloud or services providers for cloud who in turn provide service on storage for the hospitals are called private clouds who harness their treatment procedures and patient information when needed to be reviewed. The authors suggested and came up with a reliable and trustworthy architecture for EMR that assures security and privacy which can be efficient under regulated framework to access the EMR records in a private and hostile cloud[2], [13], [14].

This paper summarizes attacks on Cloud Storage and cloud communication in Sect. I conceptualizing the introduction of reviewed papers based on the problems focused, elaborating Cloud storage and Communication, focuses on need for storage over worldwide access, sections types of cloud available, describes services in cloud, list the advantages available in cloud storage, discusses possible E-health storage on cloud and lists security issues related to Cloud Communication, Sect. II elucidates literature survey by displaying the adapted method along with pros and cons of each paper surveyed, Sect. III consists of security challenges faced in cloud computing Sect.

IV explains the security practices that are and can be used overcome threats faced in cloud computing, Sect. V discusses future directions on E-Health storage and Security and Sect. VI concludes with the overview of the sections discussed on Cloud storage focused on E-Health security and the overall view of the paper.

A. Cloud Storage and Communication

The enormous growth of Electronics and digital technology is endorsed and supported in the 21st century and still in process of growth beyond imagination. Cloud computing is an internet and connection-based support that is designed by software that can store data using the services provided. It allows sharing of data resources, services, remote access etc. Cloud is a virtual storage framework which is a designed infrastructure based on the requirements. Its services are flexible according to the necessity and access. Cloud computing and its applications are reviewed and is evolving based on latest and best architecture.

B. Why the need to store data?

Data or information which are maintained by paper called as documents or hard copy that needs to be protected for a long time can deteriorate through seasons and other effects such as bugs, water and heat. Any hardware with time constraint is limited to use based on external influences such as weather, insects, etc. Information that is digitized can be stored on storage spaces, such as memory of a computer or secondary storage devices.

These devices are also bound to be corrupted by external force or severed programming that harms internal data as Viruses, malware, Trojan, etc. The access to the mentioned approach is limited as documents or hardware devices should to be carried along, this leads to the solution which is Cloud Storage. Cloud Storage is a virtual storage provided by Cloud Service providers (CSP), to store our digitized documents that can be accessed from any part of the world through internet. CSP holds warehouse servers for public use under contract with terms of use for anyone who requests Virtual storage facility.

Thus, cloud computing has become a common and buzz worthy concept in this 21st century. The introduction of Amazon web services by 2002 provided Cloud services such as storage, computation, online purchase and Artificial Intelligence.

C. Types of Cloud

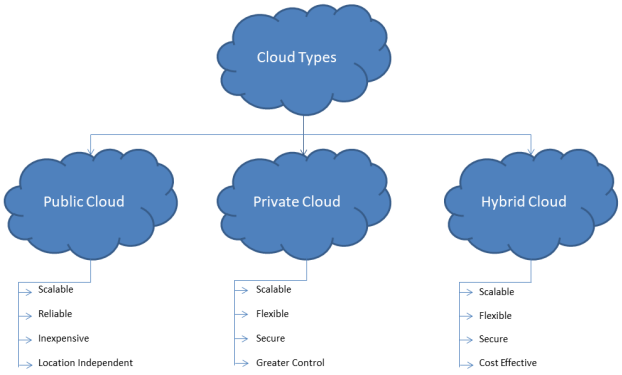

Fig. 2. Types of Cloud

Cloud is categorized or colonized under three types, Public Cloud, Private Cloud and Hybrid Cloud as shown in Figure 2, each cloud infrastructure varies accordingly based on its requirement and uses.[15].

a. Private Cloud: Private Cloud is storage for private and personal use.[2], [16]. It is an internal network that works within the organization and provides facilities within the firm's users unlike for public access. Some of the private clouds are created by organizations that are deprived access to prevent data overload and common access such as organizations with private servers for private cloud, e.g., Hospitals, Educational Institutions, organizations, companies, etc.

b. Public Cloud: It stands for its name as it is Public and extended for distributed access [2], [16], where users share and have access in the network under multiple organizations with internet connection such as Microsoft Azure, Google Cloud, Amazon Elastic Compute Cloud, etc. This cloud is managed, handled, controlled and operated by organizations that work under business forum, educational institutions, and government bodies. With respect to E-Health on Cloud computing, every organization with Cloud service such as Multispecialty hospitals, Laboratories that have stored their digital data in cloud can access stored information from any part of the world with valid credentials.

c. Hybrid Cloud: Public cloud and Private cloud merged together forms Hybrid cloud which is shown in the Figure 3 [16], data access can be done using On-Premises cloud along with public and private cloud or even between clouds which is cost effective and flexible infrastructure. It gives an optimal cloud computing environment where workloads can be moved and carried anywhere possible with access to cloud and internet.

D. Services in Cloud

Cloud computing and communication offer a wide range of services, where the three main services provided by cloud are Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) as in Figure 3.

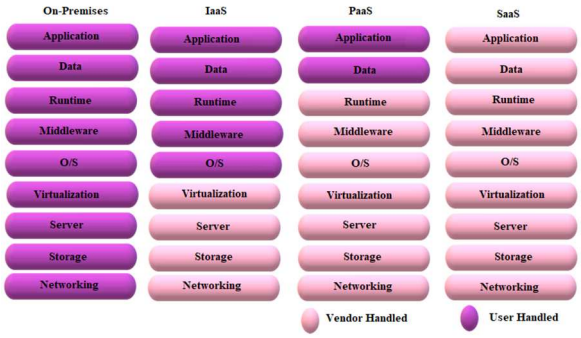

Fig. 3. Architecture of Cloud

- *Infrastructure as a Service* (IaaS) [17] also known as Hardware as a Service, is cloud service layers and platform which provide high level Application Programming level Interface (API), it delivers computational efficiency, networking resources based on demand and storage for consumers. Services can be increased or decreased grounded upon users and their computational efficiency that is required

and targeted on demanded resources which in turn reduces unnecessary up-scaling of infrastructure.

- *Platform as a Service* (PaaS) [17] is provided by cloud partner which is used for development of structure or environment that can be accessed in which the development of platform can be deployed. It is an enterprise application with is cloud enabled where it delivers everything based on the resources from simple cloud to sophisticated applications on cloud.
- *Software as a Service* (SaaS) [10], [17] is a distributed model of software where host applications use cloud provider in order to access over the internet. Any cloud service providers such as a third-party cloud provider can allow host application which is an independent software vendor that links and bridges itself between users to access the required documents or purchase anything from the cloud.

E. Advantages of Cloud

Every organization has switched their documentation services to digital cloud services along with booming technology and ideas for security and growth of company [11], [18]. Few advantages of cloud computing are Data Security, Backup and Restore, Excellent Accessibility, Improved Collaboration, Low Maintenance, Services Pay Per Use, Unlimited Storage and Mobility.

F. E-Health Storage on Cloud

Healthcare is revolutionized and reformed by could computing where abstracted document is accessed and utilized from organizations own cloud platform or from third party who has specific infrastructure and regulated services provided [19]–[21]. This evolution of document storage in digital format has turned down the possibility of physical storage space that has been stacking up documents for years together in order to re-search or to refer past medical practices or patients' history that would be used for future works resulting in elimination of error possibilities and come up with solution and idea or prefer the best solution from previous data [6], [11], [12]. The general and basic cloud services provided by the providers are as follows which form the main objectives such as Availability, Integrity, Confidentiality, Authentication and Accountability [17], [22].

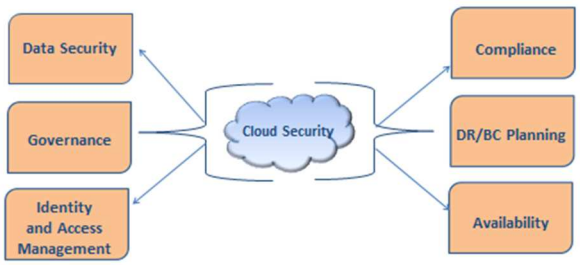

Fig. 4. Security in Cloud

G. Security Issues in Cloud Storage

The most common enterprise uses of storing data are cloud storage with security and privacy, it is cost effective than using on-premises software and hardware that can be accessed far and wide using any device, but a huge potential security risk comes along with any digital technology before raising the bar. The risks involving security on cloud storage are many but can be dealt by updating security updates frequently. Few security threats are listed as shown in figure 4 [13], [16], [26].

II. Literature Review

This section reviews papers that are taken as references from multiple forums such as Journals, Information approved by authorized personal on the internet, Books, Conference proceedings from different research service providers such as IEEE, Egyptian Journal, Symmetry, Springer, Elsevier, Research gate etc. This section discusses the merits, demerits, benefits and applications of approach used based on the algorithm and situation used.

Wang et al, discusses asymmetric key cryptography using Identity based Encryption (IBE) to determine user's information or data requester. A cost-effective Identity based proxy Re-encryption is also used for electronic health cloud access [8]. It is seen that this approach does not follow greens paradigm, with a multi-dimensional pricing model for cloud providers.

IBPRE was found to be better than re-encryption as cryptographic mechanisms are time consuming which is based on conservative Public Key Infrastructure (PKI). It is observed that this model used could not verify its performance, which was a drawback for the authors with respect to other encryption models [34].

The author Zhu et al proposed Attribute Based Encryption (ABE), where a reliable and secure framework which prevented the access of patients from exploring the network cloud [32]. This approach follows ABE and re-encryption, which prevented the health practitioner to acquire the information of the patients without their knowledge as it is unobtainable to access in the absence of read keys. The merits of this approach are that it has reduced computational overhead.

Instead of using cryptographic encryption Karakiş et al, used steganographic approach to detain the access of cloud from unauthorized personal [35]. The method was implemented by choosing image pixels in a non-sequential manner at Least Significant Bit for selection process. This method's performance was evaluated using the Mean Square Error, Peak Signal-to-Noise Ratio, Structural Similarity Measure, Universal Quality Index, and Correlation Coefficient.

Based on the findings, the proposed approach assured information security and privacy while simultaneously increasing data repository size. The drawback of this approach is that it could not handle and tackle noise cancellation and data reduction which might enhance embedding capability [36].

Kim et al [37], discussed collaborative health system, provided by Multiple Health care systems using Attribute Based Encryption (ABE), in which this paper proposes ABE for a multilevel, multilayered access by a unique collaborative E-Health system that allows for tiered data sharing while maintaining privacy (MPPDS). This method provides a more accurate statistics with meager trusted data users. The

disadvantage of this approach is that it is not scalable and flexible for users in multilayered network [38].

This paper by Chenthara et al [26], enumerates the attack faced by internal conflicts from authorized credentials within the organization, with permission to access data without alarm. Mechanisms based on comprehensive security for Electronics Health Records are discussed and explored with multiple techniques that are implemented to maintain and retain patient's information with integrity and Confidentiality.

Yeh et al, came up with an access control framework for cloud that works with fine-grained access to health and personal information of the patient which is focused on Internet of things devices that is lightweight with auditing and revocation functions for dynamic data depending on attribute [13], [37], [39]–[42]. There are multiple ciphertext policies used, where Fine-grained access control, dynamic and efficient data auditing, group auditing, and revocation are all supported by attribute-based encryption (ABE), Merkle Hash tree, and dual encryption. This method avoids fines caused by data losses on cloud by CSP that help multiple data accesses and also provides security analysis and compares performances which result with high efficiency but this system is not scalable and flexible as anticipated [43].

Attribute Based Encryption provides sharing of attributes between multiple users, revocation of a single attribute from a user influences revocation of attributes for every user in the network. Li et al. presents a Ciphertext-policy Attribute-based Encryption technique (CP-ABE) [39], [44], it formulizes a definition and defines a security model in which attribute revoked users cooperate with existing users to isolate collusion attack [45]. Using this method, a ciphertext policy for user collision avoidance is created alerting the other existing users through which the attribute group is exploited [46]. The group manager alerts the other users about the revocation of the attribute by which the remaining users are not affected. This method reduced to computational complexity of Diffie-Helman Assumptions and alerts other users about collision but it is limited as number of users increases the latency also increases.

Decentralized Key Policy Attribute Based Encryption (KP-ABE) is introduced for ensuring privacy and preserving security by Rahulamathavam et al [47], this scheme is used to avoid user collusion and to preserve privacy, however the vulnerability of this paper is that collusion attack is still present that resulted in a new scheme that is a privacy conserving decentralized KP-ABE is proposed by Zhang et al[48].

This new technique then avoids any existing linear assaults and archives the user's collision avoidance; it also demonstrates that security is limited to the decisional bilinear Deffie-Hellman assumption. The efficiency and validity are high and trusted but the disadvantages in this paper is with a greater number of users the collision attack cannot be avoided [49].

Health information storage system stores medical images that are encrypted and watermarked. To retrieve the original image the watermark has to be removed and decrypted which is not fully recoverable. A watermark an encrypted image processing technique is used that can recover the original image based on security and privacy of medical images proposed in this paper by Kester at al [50]. Using this scheme is found to be secure and authentic original medical images. The disadvantage of this framework is limited to images, as by not accepting mathematical sections, audio, text and video file.

This paper discusses on how to avoid Keyword Guessing Attack (KGA). When a search is done using Public Key Encryption Search (PKES) [51], it recognizes and retrieves the ciphertext by not reveling the secret information form cloud. However, some untrusted cloud servers are vulnerable to KGA attack that results in information leakage. Zhou et al [36], proposed and designed a Searchable Public-Key Encryption with Cryptographic Reverse Firewalls (SPKE-CRF). This protocol is found to resist KGA attack, Chosen Keyword attack (CKA) and also Algorithm Substitution Attack (ASA) using and implementing on channels that are not secure. The advantage and disadvantage are that this method reduces communication and computational cost but only with limited users over a distributed network.

A Good framework specifically designed for data access control to access E-Health Records was delivered by Rajeev et al, as a novel patient-centric scheme. Challenges that are focused are identified as scalability and fine-grained access therefore leverage attribute-based encryption ABE is used to secure patient health records data and encrypted to highest level. Multiple data across several security domains are evaluated in order to reduce key management complexity for users and owners, respectively. It is found to attain greater patient privacy and security performance by exploiting multiple authority ABE, however this framework is not tested in real time to claim its establishment, thus it does not guarantee efficiency of framework with respect to results. This method is also limited only with few users and the authors had failed to update this method with greater number of entities.

The availability of mobile services and multiple devices with iOS and Android devices the internet best collection agrees and guarantees adequate systematic security of data when at rest or otherwise. The more effectively these mobile gadgets are used, the more benefits they give. The structure is meant to raise the total security level under programming, which is dynamic, after identifying security and privacy as important issues for optimization [52], [53]. Gai et al, elaborates potency of this model through Android application framework to display its efficiency and applicability that is connected over the private cloud. Using this method personal information and resulting documents of treatments availed by the patient is updated by themselves without the aid of health practitioner. The disadvantage in this paper is that the complete control of the patient's information is controlled by the patient itself who possesses the access identity to upload personal and documented data which may or may not be precise [13], [54].

A voting-based technique is used in grid computing system to resist tampering; nevertheless, collision behavior makes these techniques purposeless with malicious resources that collectively tamper the execution of a job by delivering wrong results that are identical. The focus of this paper is to reduce and diminish Probability of Genuine Task Failure (PGTF) i.e., wrong output with expected constraint by designer and solve

spot checking optimization problem collusion attack on grid system subjects by Levitin et al [55]. The system performance is evaluated by an iterative method to minimize PGTF with task assignments that are limited. Uncertain attack parameters and fixed attack parameters are considered to demonstrate the proposed solution methodology for optimization problem.

The protocols in Standard Communication are modified in SCP-ECG, a computer-based Electrocardiography to secure data and access, that is permitted or denied based on role of access requester. This new update has supported the cryptographic tool used and of advantage to authorize and authenticate data requester which in-turn elevated privacy of sensitive information such as health records. Despite the efficiency this method holds a disadvantage that does not allow or support data to be stored on cloud and thus there is no real-time proof of the model to prove the working on a distributive environment submitted by Rubio et al [56].

Kahani et al, proposed to use a zero-knowledge protocol with a two-stage key access which is a public key encryption and Derived Unique Key Per Transaction (DUKPT) [24]. The advantage of this method is that it provides high number of access authentication requests however, implementation of this method is restricted to service providers and number of users.

The below Table 1 runs through literature survey on Cloud storage and its challenges. The papers were chosen based on computational challenges and approach used to address the problem. The output of the approach executed along with advantages and disadvantages are given as pros and cons in the below table.

TABLE I. SUMMERY OF REVIEWED ARTICLES

Author	Approach	Pros	Cons
Wang et al (2016)	Identity based Encryption (IBE) followed by Identity based proxy Re-encryption.	IBPRE was found to be better than re-encryption.	It is observed that this model used could not verify its performance.
Zhu et al (2019)	ABE and re-encryption.	Reduced Computational overhead.	Prevents health practitioner to acquire the information without patient's permission.
Karakiş et al (2015)	Steganographic approach.	Information security and privacy have been ensured, and the data repository has grown.	Noise cancellation and data reduction, which improve embedding capability, were not able to be handled and dealt with.
Kim et al (2019)	ABE for a multilevel, Multilayered access	Accurate statistics with meager trusted data users.	Not scalable and flexible for users in multilayered network.
Chenthara et al (2019)	Mechanisms based on comprehensive security	Retains patient's information with confidence and credibility.	Foolproof privacy is not imminent.
Yeh et al (2015)	Framework with fine-grained access and revocation functions based on attribute.	Avoids fines caused by data losses on cloud also provides security analysis and compares performances which result with high efficiency.	System is not scalable and flexible as anticipated.
Li et al (2018)	Ciphertext-policy Attribute based Encryption (CP-ABE)	Reduced computational complexity of Diffie-Helman Assumptions and also alerts other users about collision.	Limited number of users, as users increase latency also increases.
Rahulamathavam et al (2016)	Decentralized Key Policy Attribute Based Encryption (KP-ABE)	Avoid user collusion to a certain level and preserve privacy	Collusion attack is still present.
Zhang et al (2018)	Privacy preserving decentralized KP-ABE	Security attack is minimized and reduced to decisional bilinear Deffie-Hellman assumption resulting in great efficiency and reliability.	More number of users the collision attack cannot be avoided
Kester et al (2015)	Watermark an encrypted image processing technique	Found to be secure and authentic original medical images	Does not accept mathematical sections, audio, text and video files.
Kamara et al (2013)	Public Key Encryption Search (PKES)	Recognizes and retrieves the ciphertext by not reveling the secret information form cloud	Untrusted cloud servers are vulnerable to KGA attack that results in information leakage
Zhou et al (2021)	Searchable public-key encryption with cryptographic reverse firewalls (SPKE-CRF)	Resists Chosen Keyword attack (CKA), KGA and also Algorithm Substitution Attack represented as (ASA) and reduces communication and computational cost.	Limited users over a distributed network and computational cost increases when number of users increases.
Rajeev et al (2013)	ABE is used to secure patient health records data and encrypted to highest level	Attain better performance of patient's privacy and security by exploiting multiple authority ABE.	Could not be tested in real time thus does not guarantee efficiency of framework with respect to results and also limited to few users.

Author	Approach	Pros	Cons
Gai et al (2018)	Optimizing the structure of mobile devices with Android and iOS.	Patients can update documents without the aid of health practitioner	patient's information is controlled by the patient itself who possesses the access identity
Levitin et al (2019)	A voting-based technique used in grid computing system	Minimize probability of genuine task failure (PGTF)	Technique is ineffective due to collision behavior and produces wrong results for identical data.
Rubio et al (2013)	A redesigned SCP-ECG	Elevated privacy of sensitive information	Could not be stored on cloud thereby limits working on a distributive network.
Kahani et al (2016)	Key encryption with two stages and DUPKT protocol.	Low latency in response time with parallel and multiple user access	Not flexible and limited to number of users and limited CSP

III. SECURITY CHALLENGES IN CLOUD COMPUTING

Some of the security challenges faced in cloud computing are Lack of control, where when a private cloud is leased by organizations for its cloud services, it does not possess complete control of the services provided. An established agreement on the hardware, software and its applications are needed to establish control and trust. Lack of Visibility and shadowing, strong policies are needed to avoid new spin up instances in the SaaS environments as subscribing to new cloud services could obtain unauthorized occurrences.

Data transmission and Reception, play a vital role in securing cloud data as it is designed through Application Programming Interface (API), that often integrates and interfaces database, applications and its services. Default credentials stored on cloud also instigates vulnerability as hackers could crack into the credentials that are guessable. SaaS in cloud be incompatible based on the tools it is architectured. Incompatibilities increases risk by exposing control gaps, misconfiguration, privileged access which lead to data leaks.

Multitenancy also increases concerns in privacy as they may be more flexible than expected due to low-cost structures and shared resources. Cloud service console administrators enables management of services and privileges of cloud, provisions made flexible according to applications, configure and manage servers in a massive scale which is scalable and erasable as well. Thus, being scalable doesn't meet both ends which is compromising based on availability. External attacks such as malware attacks, firewalls, vulnerability management and treat analysis disrupts the foundation in security which leads to access cloud without much resistance. Insider related threats are unidentified for a longer period as the threat lies within the frameworks making it longest to resolve it. The above-mentioned issues and challenges are faced by cloud and its management which can be addresses according to its requirement but as flexibility and scalability increases, security also keeps cutting on both sides.

IV. SECURITY PRACTICES TO OVERCOME THRETS

Though cloud computing is can to be vulnerable to threats, it is still secure based on the practices used to eliminate attacks, some of the best practices are Network segmentation, where under shared resources which are multi-tenant environments, recourses can be shared between customers, from various organizations and firms which falls under asset segmentation. Policies and strategies should be holistic and should account for ownership and accountability leading to protection in gaps created.

Access management based on Identity and privileges provided a robust retrieval of data when requested. This provides authorized users to deliberately access services, applications, data and environment. Restricting unprivileged access increases security such as role-based attributes and continuous session monitoring ensure security and privacy of cloud access.

Grouping of asset services and instances and bringing them under specific management also increases security eliminating shadowing of IT. Controlling shared passwords also hold security authenticating systems for sensitive areas. This forms best practice in when shared passwords are controlled. Some others security practices are vulnerability management that regularly audits, scan and software patches. Encryption is one of the major aspects that ensures safety of data in cloud. Some of the best encryption system can be used to avoid loss and visibility of data. Any system is never perfect without continuous monitoring, accessing and reporting. Regular activity check, alerting and reporting decreases and detects instances occurring in the cloud due to vast access. By monitoring rigorously, a holistic environment is created minimizing and further more eliminating security threats in cloud computing.

Loss of data on cloud is also an important aspect that can be avoided by backing up data on a regular basis. Security can also be improved by using anti phishing training and two factor authentication

V. FUTURE DIRECTIONS ON E-HEALTH SECURITY

Electronic health cloud, private health cloud, electronic medical storage is clouds-based storage, which is focused on security and privacy by securing data that is uploaded on cloud by maintaining and enhancing efficiency following various strategies implementing then to find out which is the best method to attain the required motive. Security and privacy do not hold just to words that comprises of data Availability, Confidentiality, Integrity, Authenticity, etc.

Reference papers chosen for this survey is based on the research that provided various solutions for e-health Services such as types of encryption scheme used to achieve expected form of security and privacy everywhere. Most solutions used at a data encryption is known for excellent security that ensures privacy in e-health. However, the computational cost and decrypted data that is encrypted is affecting the performance of

operation to retrieve the original information. Attribute based access control is another form of method that is used to attain flexibility and scalability with patient records and effective retrievable process using authentication and authorization [57].

Based on the review conducted it is found that every review and methodology for all existing models are far from perfect and face challenges anyway[58]. Most models lack scalability, interoperability, flexibility, compatibility, and imperfect model evaluation inability to survive in a distributed environment such as cloud computing, which holds key management, computational cost, complexity is based on time, and infrastructure software and platform design for security and privacy in E-Health solutions.[59].

The significant risks in cloud storage are the procedures involved in securing and retrieving data with authenticity that is extensively sensitive that are stored on private servers. The problems faced in this research are 1. Process in securing the data based on multiple steps and procedures, 2. Encryption system that used to encrypt and decrypt confidential data, 3. Process to prove the authenticity of the data requester and as well as the information uploader, whether the uploaded sensitive data is validated and verified before it is loaded to cloud, and 4. Retrieval of the data from the requester end, provided the data requester is permissioned and authenticated.

Thus, future directions to secure Electronic Health records or patients medical records in a cloud be private, public or hybrid cloud is that it is secure in every aspect by focusing on the trust of patient's reliance, where a multi-level authentication process can be configured to retain access of documents. Also, by employing artificial intelligence and big data analytics, personalization of data can be incorporated to control the information flow and access from any part of the world. Keeping the data in track by using advisable and relevant programs could eliminate breach in the system.

Blockchain technology is a booming technology that is found to be highly secure, considering it and choosing a decentralized blockchain data can be protected by required consensus algorithms and smart contract that would suit the specific application, a permissioned blockchain would suffice the earnest search of security and privacy attainment not just for health records but also for security of any document in that aspect such as property documents, government storing information's such as Ration card, driving license, Aadhar card, Smart card, pan card, etc., tracking of goods from origin to delivery can be found and stored that is used to eliminate the spoilt goods and keep track of valid consumables.

VI. Conclusion

Healthcare is adapting and evolving digitally, where solution based on cloud stored Electronic Health Records[16], [60], [61], is fetching enough attention worldwide which has a wide impact in delivering solutions to unreachable places using internet everywhere[12], [61]–[62]. The focus on security and privacy is a demanding entity which has opened research provisions beyond borders and still on finding an ideal method to attain security and privacy on Cloud based EHR. The existing methods such as Attribute Based Encryption, RSA algorithm, Identity Based Encryption (IBE) efficient, Identity Based Proxy Re-encryption (IBPRE) schemes, Access Control policy, Re-encryption and Attribute Based Encryption (ABE), Role Based Access Control (RBAC), Enhanced Role Based Access Control model (RBAC), fine grid computing system and distributed task for optimization. So, to safeguard the digitized health data an appropriate solution is to upgrade a delegate layer of information between sensor hubs and cloud that can be transmitted along with a well accessed framework. Despite various advantages in cloud computing, it is relevant and efficient to utilize cloud to its full potential. It is concluded that it is appropriate only if solution developed specifically for security that safe guard's patient information by maintaining it. It is better to have a file-based security along with cloud specific security increasing the flexibility and scalability of cloud without compromising its required and basic specifications.

References

[1] J. Wang, X. Chen, J. Li, J. Zhao, and J. Shen, "Towards achieving flexible and verifiable search for outsourced database in cloud computing," Future Generation Computer Systems, vol. 67, pp. 266–275, 2017, doi: 10.1016/j.future.2016.05.002.

[2] Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan, and G. Fortino, "An improved authentication scheme for remote data access and sharing over cloud storage in cyber-physical-social-systems," IEEE Access, vol. 8, pp. 47144–47160, 2020, doi: 10.1109/ACCESS.2020.2977264.

[3] W. Shen, B. Yin, X. Cao, Y. Cheng, and X. Shen, "A distributed secure outsourcing scheme for solving linear algebraic equations in Ad Hoc clouds," IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 415–430, 2019, doi: 10.1109/TCC.2016.2647718.

[4] Y. Wu, Y. Lyu, and Y. Shi, "Cloud storage security assessment through equilibrium analysis," Tsinghua Science and Technology, vol. 24, no. 6, pp. 738–749, 2019, doi: 10.26599/TST.2018.9010127.

[5] P. Zhang, M. Zhou, and Y. Kong, "A Double-Blind Anonymous Evaluation-Based Trust Model in Cloud Computing Environments," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 3, pp. 1805–1816, 2021, doi: 10.1109/TSMC.2019.2906310.

[6] R. Gajanayake, R. Iannella, and T. Sahama, "Privacy oriented access control for electronic health records," Electronic Journal of Health Informatics, vol. 8, no. 2, 2014.

[7] Gkoulalas-Divanis and G. Loukides, Medical data privacy handbook, no. January. 2015. doi: 10.1007/978-3-319-23633-9.

[8] A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," Future Generation Computer Systems, vol. 67, pp. 242–254, 2017, doi: 10.1016/j.future.2016.08.008.

[9] H. S. Gardiyawasam Pussewalage and V. A. Oleshchuk, "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions," International Journal of Information Management, vol. 36, no. 6, pp. 1161–1173, 2016, doi: 10.1016/j.ijinfomgt.2016.07.006.

[10] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach," Future Generation Computer Systems, vol. 43–44, pp. 99–109, 2015, doi: 10.1016/j.future.2014.08.010.

[11] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," Symmetry, vol. 13, no. 5, 2021, doi: 10.3390/sym13050742.

[12] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," Egyptian Informatics Journal, vol. 20, no. 2, pp. 97–108, 2019, doi: 10.1016/j.eij.2018.12.001.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013, doi: 10.1109/TPDS.2012.97.

[14] K. Lee, "Comments on 'Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption,'" IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1299–1300, 2020, doi: 10.1109/TCC.2020.2973623.

[15] K. A. Torkura, M. I. H. Sukmana, F. Cheng, and C. Meinel, "CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure," IEEE Access, vol. 8, pp. 123044–123060, 2020, doi: 10.1109/ACCESS.2020.3007338.

[16] Rezaeibagha and Y. Mu, "Distributed clinical data sharing via dynamic access-control policy transformation," International Journal of Medical Informatics, vol. 89, no. February 2016, pp. 25–31, 2016, doi: 10.1016/j.ijmedinf.2016.02.002.

[17] M. Zhou, R. Zhang, D. Zeng, and W. Qian, "Services in the cloud computing era: A survey," 2010 4th International Universal Communication Symposium, IUCS 2010 - Proceedings, pp. 40–46, 2010, doi: 10.1109/IUCS.2010.5666772.

[18] J. Chase, D. Niyato, P. Wang, S. Chaisiri, and R. K. L. Ko, "A Scalable Approach to Joint Cyber Insurance and Security-As-A-Service Provisioning in Cloud Computing," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 4, pp. 565–579, 2019, doi: 10.1109/TDSC.2017.2703626.

[19] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018, doi: 10.1109/ACCESS.2018.2852784.

[20] L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang, "An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing," IEEE Access, vol. 6, no. c, pp. 19025–19033, 2018, doi: 10.1109/ACCESS.2018.2819166.

[21] L. Fan et al., "c," The International Conference on eHealth, Telemedicine, and Social Medicine, eTELEMED, no. 4, pp. 98–104, 2012.

[22] Anglano, R. Gaeta, and M. Grangetto, "Securing coding-based cloud storage against pollution attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 28, no. 5, pp. 1457–1469, 2017, doi: 10.1109/TPDS.2016.2619686.

[23] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems," IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4101–4112, 2018, doi: 10.1109/TII.2018.2832251.

[24] N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and Access Control in e-Health Systems in the Cloud," Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S, no. August, pp. 13–23, 2016, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.43.

[25] S. R. Rathi and V. K. Kolekar, "Trust Model for Computing Security of Cloud," Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018, pp. 1–5, 2018, doi: 10.1109/ICCUBEA.2018.8697881.

[26] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," IEEE Access, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[27] L. Ogiela, "Cryptographic techniques of strategic data splitting and secure information management," Pervasive and Mobile Computing, vol. 29, pp. 130–141, 2016, doi: 10.1016/j.pmcj.2015.05.007.

[28] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 1, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.

[29] Yan, Gongjun, Ding Wen, Stephan Olariu, and Michele C. Weigle. "Security challenges in vehicular cloud computing." IEEE Transactions on Intelligent Transportation Systems 14, no. 1 (2012): 284-294.

[30] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," IEEE Access, vol. 7, no. c, pp. 9368–9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[31] L. Zhang, N. Yin, J. Liu, and R. Wang, "Collusion detector based on G-N algorithm for trust model," Journal of Systems Engineering and Electronics, vol. 27, no. 4, pp. 926–935, 2016, doi: 10.21629/JSEE.2016.04.22.

[32] L. Zhu, M. Li, and Z. Zhang, "Secure fog-assisted crowdsensing with collusion resistance: From data reporting to data requesting," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5473–5484, 2019, doi: 10.1109/JIOT.2019.2902459.

[33] Y. Hu, J. Chen, and S. Zhang, "Collusion Trap Against GVW'13 ABE," IEEE Access, vol. 7, pp. 36334–36339, 2019, doi: 10.1109/ACCESS.2019.2904846.

[34] Z. Yan, R. H. Deng, and V. Varadharajan, "Cryptography and Data Security in Cloud Computing," Information Sciences, vol. 387, pp. 53–55, 2017, doi: 10.1016/j.ins.2016.12.034.

[35] R. Karakiş, I. Güler, I. Çapraz, and E. Bilir, "A novel fuzzy logic-based image steganography method to ensure medical data security," Computers in Biology and Medicine, vol. 67, pp. 172–183, 2015, doi: 10.1016/j.compbiomed.2015.10.011.

[36] Y. Zhou, Z. Hu, and F. Li, "Searchable Public-Key Encryption with Cryptographic Reverse Firewalls for Cloud Storage," IEEE Transactions on Cloud Computing, vol. 7161, no. c, pp. 1–1, 2021, doi: 10.1109/tcc.2021.3095498.

[37] J. W. Kim, K. Edemacu, and B. Jang, "Mppds: Multilevel privacy-preserving data sharing in a collaborative ehealth system," IEEE Access, vol. 7, pp. 109910–109923, 2019, doi: 10.1109/ACCESS.2019.2933542.

[38] T. Halabi and M. Bellaiche, "Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach," IEEE Transactions on Cloud Computing, vol. 8, no. 3, pp. 928–942, 2020, doi: 10.1109/TCC.2018.2820715.

[39] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User Collusion Avoidance CP-ABE with Efficient Attribute Revocation for Cloud Storage," IEEE Systems Journal, vol. 12, no. 2, pp. 1767–1777, 2018, doi: 10.1109/JSYST.2017.2667679.

[40] M. RajeevKumar, M. Dhilsath Fathima, and M. Mahendran, "Personal Health Data Storage Protection on Cloud Using MA-ABE," International Journal of Computer Applications, vol. 75, no. 8, pp. 11–16, 2013, doi: 10.5120/13129-0490.

[41] L. Y. Yeh, P. Y. Chiang, Y. L. Tsai, and J. L. Huang, "Cloud-Based Fine-Grained Health Information Access Control Framework for LightweightIoT Devices with Dynamic Auditing andAttribute Revocation," IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 532–544, 2018, doi: 10.1109/TCC.2015.2485199.

[42] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," Future Generation Computer Systems, vol. 78, pp. 1020–1026, 2018, doi: 10.1016/j.future.2016.12.027.

[43] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," Electronics (Switzerland), vol. 8, no. 7, pp. 1–49, 2019, doi: 10.3390/electronics8070768.

[44] H. Y. Lin and Y. R. Jiang, "A multi-user ciphertext policy attribute-based encryption scheme with keyword search for medical cloud system," Applied Sciences (Switzerland), vol. 11, no. 1, pp. 1–14, 2021, doi: 10.3390/app11010063.

[45] Hyla, Tomasz, and Jerzy Pejaś. "Demonstrably Secure Signature Scheme Resistant to ${k} $-Traitor Collusion Attack." IEEE Access 6 (2018): 50154-50168.

[46] Y. Liu and N. Li, "Retrieving hidden friends: A collusion privacy attack against online friend search engine," IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 833–847, 2019, doi: 10.1109/TIFS.2018.2866309.

[47] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, "User Collusion Avoidance Scheme for Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Computers, vol. 65, no. 9, pp. 2939–2946, 2016, doi: 10.1109/TC.2015.2510646.

[48] L. Zhang, P. Liang, and Y. Mu, "Improving privacy-preserving and security for decentralized key-policy attributed-based encryption," IEEE

Access, vol. 6, pp. 12736–12745, 2018, doi: 10.1109/ACCESS.2018.2810810.

[49] P. S. Wang, F. Lai, H. C. Hsiao, and J. L. Wu, "Insider Collusion Attack on Privacy-Preserving Kernel-Based Data Mining Systems," IEEE Access, vol. 4, pp. 2244–2255, 2016, doi: 10.1109/ACCESS.2016.2561019.

[50] Q. A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, "A Security Technique for Authentication and Security of Medical Images in Health Information Systems," Proceedings - 15th International Conference on Computational Science and Its Applications, ICCSA 2015, pp. 8–13, 2015, doi: 10.1109/ICCSA.2015.8.

[51] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7859 LNCS, pp. 258–274, 2013.

[52] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things," Future Generation Computer Systems, vol. 85, pp. 190–200, 2018, doi: 10.1016/j.future.2018.03.043.

[53] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," Proceedings - IEEE INFOCOM, vol. 2016-July, pp. 1–9, 2016, doi: 10.1109/INFOCOM.2016.7524606.

[54] M. Barua, X. Liang, R. Lu, and X. Shen, "Ontario Graduate Scholarship (OGS) in 2007, R.S. McLaughlin Fellowship in 2008, Natural Sciences and Engineering Research Council of Canada Graduate Scholarships in 2009, and President's Graduate," Int. J. Security and Networks, vol. 6, no. 3, pp. 67–76, 2011.

[55] G. Levitin, L. Xing, and Y. Dai, "Optimal Spot-Checking for Collusion Tolerance in Computer Grids," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 2, pp. 301–312, 2019, doi: 10.1109/TDSC.2017.2690293.

[56] Óscar J. Rubio, Álvaro Alesanco, and J. García, "A robust and simple security extension for the medical standard SCP-ECG," Journal of Biomedical Informatics, vol. 46, no. 1, pp. 142–151, Feb. 2013, doi: 10.1016/j.jbi.2012.07.007.

[57] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016, doi: 10.1109/TPDS.2015.2401003.

[58] P. H. Vilela, J. J. P. C. Rodrigues, R. da R. Righi, S. Kozlov, and V. F. Rodrigues, "Looking at fog computing for e-health through the lens of deployment challenges and applications," Sensors (Switzerland), vol. 20, no. 9, pp. 1–26, 2020, doi: 10.3390/s20092553.

[59] S. Islam, M. Ouedraogo, C. Kalloniatis, H. Mouratidis, and S. Gritzalis, "Assurance of Security and Privacy Requirements for Cloud Deployment Models," IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 387–400, 2018, doi: 10.1109/TCC.2015.2511719.

[60] Dubovitskaya, Alevtina, Visara Urovi, Matteo Vasirani, Karl Aberer, and Michael I. Schumacher. "A cloud-based ehealth architecture for privacy preserving data integration." In IFIP International Information Security and Privacy Conference, pp. 585-598. Springer, Cham, 2015.

[61] Jaishree Jain and Dr. Ajit Singh, "A Survey on Security Challenges of Healthcare Analysis Over Cloud," International Journal of Engineering Research and, vol. V6, no. 04, pp. 905–912, 2017, doi: 10.17577/ijertv6is040719.

[62] J. Hanen, Z. Kechaou, and M. Ben Ayed, "An enhanced healthcare system in mobile cloud computing environment," Vietnam Journal of Computer Science, vol. 3, no. 4, pp. 267–277, 2016.