International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.8, August 2015 DOI:10.15693/ijaist/2015.v4i8.113-118

Survey Of Major Access Control Approaches For Health Records In Cloud

Lakshmi Mohanan
PG Scholar/Computer Science Department
Adi Shankara Institute Of Engineering and Technology, Kalady, India

Ajay Basil Varghese
Assistant Professor/IT Department
Adi Shankara Institute Of Engineering and Technology, Kalady, India

***Abstract*—The widespread adoption of Personal Health Records (PHR)/Electronic Health Records (EHR) has greatly improved the quality of healthcare systems world over. Cloud computing with its storage scalability and cost effectiveness has been the driving force technology behind this shift. Since usage of cloud for healthcare involves entrusting the patient health records to cloud providers, there are increased concerns of safety and security of outsourced health data. Many approaches including cryptographic and non cryptographic techniques have been suggested to ensure the privacy of health records stored and exchanged using cloud. This paper categorizes the several access control approaches that have come about in cloud to protect health records residing in cloud. We also highlight the major advantages and the shortcomings of these different category of approaches.**

Index terms –health records, access control, cryptography, cloud, encryption.

I. INTRODUCTION

The health care is one among the world's largest and fastest-growing sectors, providing life saving goods and services to patients. This industry has a never ending focus on finding more effective, efficient and affordable ways to provide high quality and accessible health services to all. Information technology applied to healthcare, termed Health IT (HIT) has opened the door towards better quality patient care through the secure use and exchange of health information. It also provides a system for patients to manage and share their health history effortlessly. HIT includes the use of electronic health records (EHRs) and personal health records (PHR) instead of paper medical records to maintain patient health information. The PHRs and EHRs, are both electronic versions of patient medical history. The PHRs are controlled by patients themselves [1]; while, the EHRs [2] are managed by the healthcare providers. American Recovery and Reinvestment Act (ARRA) [27] stipulates that all healthcare organizations must implement the use of electronic health records by 2015. Furthermore Health Insurance Portability and Accountability Act (HIPAA) [28] mandates certain physical, network, and process security measures that needs to be in place and followed to ensure confidentiality and integrity of health data. If these mandates are not satisfied, penalties will ensue. Therefore, as the law mandates, healthcare professionals will have to digitalize their work.

Cloud computing is the technology that has played a pivotal role in modernizing the healthcare industry. Cloud computing, is the delivery of on-demand computing resources, everything from applications to data centers to IT infrastructure—over the internet on a pay-per-use basis. It enables companies to consume computing resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house. Traditionally digitization in the healthcare was done using in-house infrastructure with dedicated resources managing and maintaining them. This creates huge overhead for the healthcare providers that can diminish the benefits of IT for them. Cloud computing can bring in a change here by providing an infrastructure that allows hospitals, medical practices, insurance companies, and research facilities to tap improved computing resources at lower initial capital outlays.

However healthcare data has stringent requirements for security, confidentiality, availability to authorized users, traceability of access, reversibility of data, and long-term preservation along with the need to conform to government and industry regulations like HIPAA and ARRA. While cloud services can offer advanced technical solutions at an attractive price compared to on premise hardware and software, issues of privacy and security are also very different for healthcare. Storing the patient health data in the third-party servers can endanger the security and privacy of this data.

This paper aims to study the different access control mechanisms proposed for health records in cloud. Studies on access control mechanisms started by early 1960's and 1970 and the most prominent among the earlier schemes were Bell-La Padula (BLP) [3] and BiBa [4] models. All these early models were applicable only to scenarios where the data owner and consumer are within the same trusted domain, and is hence unsuitable for a cloud environment. Further to that several access control mechanisms including both cryptographic and non cryptographic methods were proposed. Non cryptographic techniques can never be truly secure in public clouds and are prone to information disclosure to insiders. The categories of cryptographic techniques proposed are Public Key Encryption (PKE) based approaches, Symmetric Key Encryption (SKE) based approaches and Attribute Based Encryption (ABE) approaches. Among these, ABE schemes are more suitable for cloud environment in proving fine grained access control.

II. RELATED WORK

The major approaches for access control in cloud may be categorized into

1. Cryptographic approaches.
2. Non-cryptographic approaches.

Cryptographic approaches use some advanced forms of cryptography for encrypting the data like PKE, SKE, ABE and the likes. On the other hand non-cryptographic approaches utilize policy based authorization for enforcing access control. These schemes may also use certain primitive cryptographic techniques like hash functions or digital signature verification. A graphical representation of the different approach categories for access control are represented in Fig. 1.1. A detailed explanation of these approach categories are given in the subsequent sections.

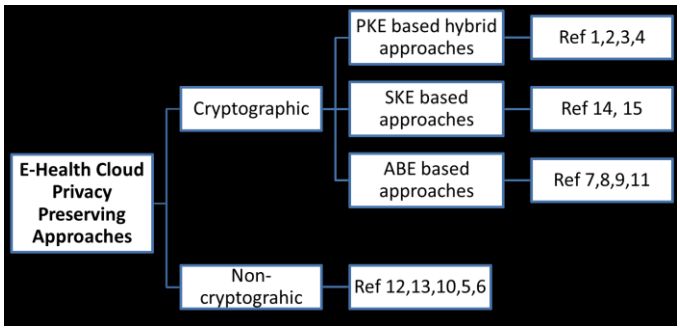

Figure 1.1 Category of Access Control Approaches

A. Non Cryptographic Approaches

Quite a few non-cryptographic approaches have been proposed to preserve privacy of health data in the cloud. These approaches mainly use certain policy-based authorization that allows the data objects to have access control policies. Some of the aforementioned systems also use few cryptographic primitives, such as hash functions and digital signature verification. Below, are the major non-cryptographic approaches for preserving privacy in the e-Health cloud.

Kamran et al. proposed [5] a watermarking scheme for right protection of EMR systems. The method computes a watermark that when inserted into the EHR does not alter its vital/diagnostic features hence preventing misdiagnosis. Decoding the watermark is done using majority voting, based on a novel watermark decoder. This method of decoding is resilient to insertion, deletion and alteration attacks. Currently this method is limited to only numeric values and calculating the watermark for each feature requires multiple iterations through the full database, which can prove costly for a huge medical database. SparkMed [6] is framework for dynamic Integration of multimedia medical data into distributed m-Health System proposed by Kim. Integrates techniques from multimedia streaming, rich Internet applications (RIA), and RPC to construct a Self-managing, Pervasive Automated netwoRK for Medical Enterprise Data (SparkMed). Individual SparkMed daemons can attach to any non-networked medical software processes without significantly impacting their performance. While proving a medical data cloud, it lacks full QoS and data synchronization in a browser based environment. Continuous synchronization of huge and unused data can consume unnecessary resources.

Secure health data application software based on virtual machines is presented in [7] called MyPHRMachines. After uploading the PHRs on MyPHRMachine, the patient access the PHRs through Virtual Machine (VM) to delegate the access rights selectively to individual caregivers. The patients can also monitor the PHRs through the remote desktop protocol and shutdown the VM session if they realize a misuse of PHR data. On the downside this technique can lead to numerous personal application islands, in which each patient collects heterogeneous PHR data and application software and lack of internet access for the VMs in which the data and software prevents it from accessing other web services. DACAR [8] platform by Fan et al. facilitates the development of ehealth services by providing secure platform as a service. But this makes the applications that are developed on the predefined platform rather inflexible in terms of security. Any additional security or modifications to the existing protection techniques will be difficult to implement.

B. Cryptographic Approaches

The cryptographic approaches commonly used in the e-Health cloud-based systems to protect data use schemes, such as Public Key Encryption (PKE) and Symmetric Key Encryption (SKE). Other cryptographic primitives that are also used include searchable encryption, (Hierarchical) Identity-Based Encryption (HIBE), Proxy Re-encryption (PRE), Predicate/Hierarchical Predicate Encryption (HPE), and (Fully) homomorphic encryption. In this section approaches based on PKE, SKE and ABE are described as most of the others are variations of these two basic forms.

PKE based approaches

In public key encryption otherwise known as asymmetric cryptography, each user has two separate keys; one key is private and know only to that user, while the other one is public and known to all. Although these two are different some part of them is mathematically linked together. If Alice wants to send a message to Bob using PKE, Alice encrypts the message using Bob's public key and sends it to him. On receiving the encrypted message, Bob uses his private key to decrypt it and obtain the original message. As Bob's private key is know only to him, the message cannot be read by anyone else. Hence a message encrypted using a public key can only be decrypted using its matching private key. This is depicted in Fig 1.2.

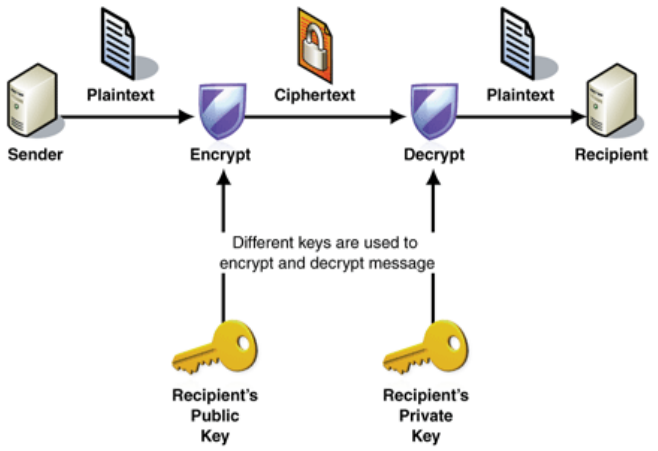

Fig 1.2 Public Key Encryption

Solutions based on the PKE are secure but using the PKE alone is computationally less efficient due to the slower operations and the larger key sizes. Therefore, the PKE is used in conjunction with the SKE where symmetric keys are used to encrypt the contents while public/private keys are used to secure the symmetric keys. The common public key algorithms use the RSA and Elliptic Curve Cryptography (ECC) techniques for generating public/private parameters used for security services. The section below presents the PKE with SKE hybrid approaches to protecting data privacy in cloud.

In the security model proposed by Liu et al. [10] a reference security model for EHR collection, storage and verification is proposed. Role based composite EHR model is used for secure collection and integration of health records. Encryption and Access Management is handled by cryptographic access control and anonymous digital credential for signature and verification. This provides ample security but key management and distribution is hard to address in cryptographic access control. [11] talks about a digital rights management approach for health record privacy. In this approach data is always in encrypted form using a content key encryption. Only users having valid license are allowed to decrypt and use the content. License is issued by content owner, policies expressed in the license are enforced by the agent, which is present on the client side. The presence of client side agent to enforce the policies increases overhead at the client side and it also lacks the capability to ensure data confidentiality and integrity.

Method for enhancing accountability of electronic health record usage via patient-centric monitoring is introduced in [12]. The proposed system architecture and related protocols that enable either explicit or implicit patient control over the health information. The records are encrypted through the PKE with corresponding hash values. To ensure the usage of record by only trusted entities, the concept of Universal Designated Verifier Signatures (UDVS) is introduced. This supports accountable usage of health records and the UDVS function used is publicly verifiable. The major drawback with this technique is that it assumes that the health data is first created by record issuers that have knowledge about the contents of records, hash values, and signatures and hence can be misused by them. The architecture for securing the e-health cloud in [13] uses the concept of Trusted Virtual Domains (TVD) to establish the access control. The TVD platforms contain the security kernel and other physical components that virtual machines may utilize to enforce the policies. The data is automatically encrypted through the PKE. When a client machine wants to connect with the TVD, the underlying infrastructure authenticates the integrity of the client platform. But this mechanism requires the patient to be online for PHR access and is not suitable for emergency situations.

SKE based approaches

Unlike PKE, SKE has the same keys for encryption as well as decryption. The sender and the receiver share one single secret key. The plaintext is encrypted using the shared symmetric key and same key is used by the receiver for decrypting the message. SKE scheme of encryption is shown in Fig 1.3. SKE is much faster computationally than asymmetric algorithms as the encryption process is less complicated. The SKE-based schemes can effectively secure data and protect its confidentiality but may require additional procedures to implement the access control. The SKE based algorithm currently in use and acting as standard is the Advanced Encryption Standard (AES). The SKE-based approaches to protect the health data in the cloud are presented below.

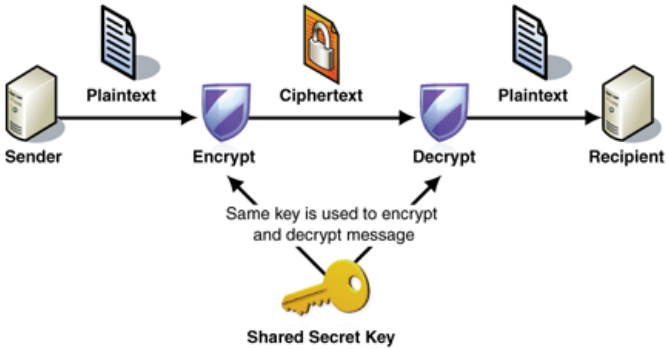

Fig 1.3 Symmetric Key Encryption

A mechanism for unlinkability between the patients and electronic medical records in the cloud environment is presented by Li et al. [16]. The patients' electronic medical records are encrypted through the SKE and are stored in an anonymous way. The doctors use digital signatures to process the patient health records after the treatment for storage at the cloud. The Electronic Medical Record number (PID), identity seed stored inside the Patients' Health Card (SID), a random value (R), and a serial number for treatment (SN) are required to access the patients' electronic medical record. Moreover, to access the heath data, a smart card is required that contains the SID.

A dynamic access structure to enforce precise access control over the PHRs in multiuser cloud environment is introduced by Chen et al. [14]. The health records are encrypted and decrypted through Lagrange multipliers using the SKE. Major advantages of this approach is the automatic revocation of the users and reduced complexities of key management. Zhang et al. has introduced a role-based and time-based access control approach in [15]. Method allows legitimate users to access EHRs for a specific period of time, based on their access roles and has got better handling of key distribution. The approach is limited in the sense that it requires a user to work in multiple roles and fine grained access is not possible using his method.

ABE based approaches

The traditional PKE approaches encrypt a message for a specific user. For Alice to send a message to Bob, there needs to be trust/familiarity between them. But in cases where one will not be able to ascertain beforehand the people who will be accessing our data, this method fails. For addressing these scenarios, we need to have a trusted third party in place, who can issue keys to users after verifying their credentials. The concept of ABE was first introduced by Sahai et al. [17]. ABE is a cryptographic primitive based on the PKE where the messages are encrypted and decrypted on the basis of attributes. The major advantage of ABE over other techniques is that it allows fine grained access control policies to be specified and enforced. Standard ABE approaches are considered as costly in terms of decryption because of bilinear computation steps. The two major categories of ABE are

1. Key Policy Attribute Based Encryption (KP-ABE)

2. Ciphertext Policy Attribute Based Encryption (CP-ABE)

In KP-ABE, the policies are specified in the users key, while the ciphertext is associated with attributes. If the attributes of the ciphertext satisfy the policy in the users key, the user can decrypt the ciphertext. But KP-ABE has the limitation that the data owner cannot specify the policy for access and can only define the attributes.

In contract to this, CP-ABE has policy associated with the ciphertext and attributes with the user's key. If the attributes in the user key satisfy the policy of the cipher, the user can decrypt the document. Both these are depicted in Fig 1.4 and Fig 1.5. The approaches based on different ABE variations are as below.

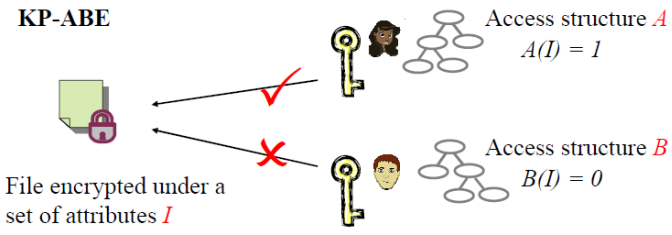

Fig 1.4 KP-ABE

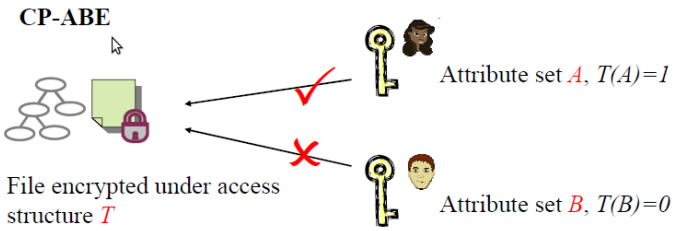

Fig 1.5 CP-ABE

In [18] Liu et al. proposes a form of attribute based encryption for scalable and secure sharing of PHR. The major feature is the use of MA-ABE for the public domains and KP-ABE for personal domains. Also provides break-glass access to PHRs under emergence scenarios. Although the use of MA-ABE in the public domain handles the key escrow problem, it does not fully utilize the scalability of cloud and user revocation and key management is not satisfactorily addressed. CAM [19] for mobile health data monitoring aims to preserve privacy of the clients and the mobile health (mHealth) service providers. The privacy of clients is protected using identity-based encryption. The method relies on homomorphic encryption while transferring the data from the mobile health provider to the cloud which is effective in performing the meaningful computations over the encrypted data. To reduce decryption complexities for clients, outsourcing decryption technique is used. This method can be used only for specific patients who needs continuous monitoring using sensor devices.

For multiauthority cloud storage DAC-MACS [20] is proposed where new multiauthority CP-ABE scheme with efficient decryption is constructed with main computation outsourced using a token-based decryption method. Provides design of an efficient immediate attribute revocation method for multiauthority CP-ABE scheme that achieves both forward security and backward security. [21] introduces a model to build privacy into mobile healthcare systems with the help of the private cloud. It integrates the concept of attribute based encryption with threshold signing for providing role based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.

The conclusion on the study of the several access control approaches above is summarized in the below Table 1.1.

Approach Category	Characteristics
Non Cryptographic Approaches	• Cannot provide true security in public cloud. • Is only suitable for private cloud.
PKE based approaches	• Computationally less efficient with larger key sizes. • Fine grained access control cant be achieved .
SKE based approaches	• Provides only confidentiality of data. • Need additional method to provide access control.
ABE based approaches	• Can achieve any desired level of privacy. • Fine grained access control possible. • Needs to handle user revocation. • Multi authority ABE most effective among the many ABE variations.

Table 1.1

III. CONCLUSION

From the above study of access control approaches in cloud for health records, it can be seen that only cryptographic approaches are suitable for health records in cloud. Among the different cryptographic variations, both PKE and SKE based approaches cannot provide fine grained access control that is critical to medical records. At the same time, the ABE based approaches can provide fine grained access control along with easy user revocation and are better suitable for the cloud environment.

.

REFERENCES

[1]. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, _A research agenda for personal health records (PHRs),_ J. Am. Med. Informat. Assoc., vol. 15, no. 6, pp. 729_736, 2008.

[2]. L. C. Huang, H. C. Chu, C. Y. Lien, C. H. Hsiao, and T. Kao, _Privacy preservation and informationsecurity protection for patients' portable electronic health records,_ Comput. Biol. Med., vol. 39, no. 9,pp. 743_ 750, 2009.

[3]. D. E. Bell and L. J. LaPadula, Secure Computer Systems: Uni_ed Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[4]. K. J. Biba, Integrity Considerations for Secure Computer Sytems The MITRE Corporation, Tech. Rep., 1977.

[5]. M. Kamran and M. Farooq, _An information-preserving watermarking scheme for right protection of emr systems,_ IEEE Trans. on Knowledge and Data Eng., Nov. 2012.

[6]. Constantinescu L, Kim J, Feng D: SparkMed: A Framework for Dynamic Integration of Multimedia Medical Data into Distributed m-Health Systems. IEEE T Inf Technol Biomed 2012, 16(1):40_52.

[7]. P. V. Gorp and M.Comuzz i, _Lifelong personal health data and application software via virtual machines in the cloud,_ IEEE J. Biomed. Health Informatics, vol. 18, no. 1, pp. 1_10, Jan. 2014.

[8]. L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, and D. Bell, _DACAR platform for e-health services cloud,_ in Proc. 4th IEEE Int. Conf. Cloud Comput., Jul. 2011, pp. 219_226.

[9]. R.Wu, G.-J. Ahn, and H. Hu, _Secure sharing of electronic health records in clouds,_ in Proc. 8th IEEE Int. Conf. Collaborative Comput., Netw., Appl. Worksharing, 2012, pp. 711_718.

[10]. R. Zhang and L. Liu, _Security models and requirements for healthcare application clouds,_ in Proc. IEEE 3rd Int. Conf. Cloud Comput., Jul. 2010, pp. 268_275.

[11]. M. Jafari,R. S.Naini, andN. P. Sheppard, _A rights management approach to protection of privacy in a cloud of electronic health records,_ in Proc. 11th Annu. ACM Workshop Digital Rights Manag., Oct. 2011, pp. 23_30.

[12]. D. Mashima and M. Ahamad, _Enhancing accountability of electronic health record usage via patient-centric monitoring,_ in Proc. 2nd ACM SIGHIT Sympo. Int. Health Informat., Jan. 2012, pp. 409_418.

[13]. L. Hans, A. R. Sadeghi, and M. Winandy, _Securing the e-Health cloud,_ in Proc. 1st ACM Int. Health Informat. Sympo., Nov. 2010, pp. 220_229.

[14]. T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, _Secure dynamic access control scheme of PHR in cloud computing,_ J. Med. Syst., vol. 36, no. 6, pp. 4005_4020, 2012.

[15]. R. Zhang, L. Liu, and R. Xue, Role-based and time-bound access and management of EHR data, Security Commun. Netw., 2013, DOI: 10.1002/sec.

[16]. Z. R. Li, E. C. Chang, K. H. Huang, and F. Lai, A secure electronic medical record sharing mechanism in the cloud computing platform, in Proc. 15th IEEE Int. Sympo. Consum. Electron., Jun. 2011, pp. 98103.

[17]. A. Sahai and B. Waters, Fuzzy identity based encryption, Adv. Cryptol. Eurocrypt, vol. 3494, pp. 457473, May 2005.

[18]. M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131143, Jan. 2013.

[19]. H. Lin, J. Shao, C. Zhang, and Y. Fang, CAM: Cloud-assisted privacy preserving mobile health monitoring, IEEE Trans. Inf. Forensics Security, vol. 8, no. 6, pp. 985997, Jun. 2013.

[20]. Kan Yang, Xiaohua Jia, Kui Ren, and Bo Zhang. DAC-MACS: Eective data access control for multi-authority cloud storage systems. In INFOCOM, 2013 Proceedings IEEE, pages 2895 2903, 2013. 2, 9

[21]. Yue Tong, Jinyuan Sun, Chow S.S.M. , Pan Li, Cloud-Assisted Mobile Access of Health Data With Privacy and Auditability , IEEE J. Biomed. Health Informatics, vol. 18, no. 2, pp. 419 - 429, Mar. 2014.

[22]. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing, Proc. IEEE INFOCOM '10, 2010.

[23]. Wan, Zhiguo, Jun E. Liu, and Robert H. Deng. "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing."Information Forensics and Security, IEEE Transactions on 7.2 (2012): 743-754.

[24]. R. Bobba, H. Khurana, and M. Prabhakaran, Attribute-sets: A practically motivated enhancement to attribute-based encryption, in Proc. ESORICS, Saint Malo, France, 2009.
[25]. http://www.healthcareitnews.com/news/phishing-scam-data-breach-compromises-data-39k.
[26]. http://www.himss.org/ResourceLibrary/genResourceDetailPDF.aspx?ItemNumber=41958.
[27]. http://www.recovery.gov/arra/About/Pages/The_Act.aspx.
[28]. http://health.state.tn.us/HIPAA/index.htm

Authors Profile

Lakshmi Mohananreceived the **B.E.** degree in computer science and engineering from the Crescent Engineering College, Chennai, Anna University, 2006.Currently doing **M.E.** in computer science and engineering in Adi Shankara Institute Of Engineering and Technology. Her research interest includes Cloud Security, Cryptography, Health care security.

Ajay Basil Varghesereceived the **B.Tech.** degree in information technology from Viswajyothi College of Engineering,M.G University, Kerala, 2010. He also received his M.E degree from Anna University, Chennai 2012.Currently holds the post of Assistant professor in Adi Shankara Institute of Technology, Kalady.His research interests include Cloud computing, Internet of things.