ENCRYPTION MECHANISM ON PATIENT 
DATA STORED IN CLOUD 

V. GOUTHAMI*1 
V. SUDHARANI*2 
DR P. NIRANJAN REDDY*3 

*1 Asst Prof, Dept of CSE Kakatiya Institute of Technology and Science 
*2 Asst Prof, Dept of CSE Aurora's Research and Technological Institute 
*3 Professor & Head Department of CSE Kakatiya Institute of Technology and Science 

Abstract—Cloud computing is a broad and diverse phenomenon. Users are allowed to store large amount of data on cloud storage for future use. The various security issues related to data security, privacy, confidentiality, integrity and authentication needs to be addressed. Among these issues security is concerned to be more serious issue. To provide data security in the cloud the data should be encrypted with standard methods and make the data more secure. In this paper we propose an encryption method which is applied on data to be stored in cloud. With respect to its service offerings, operating models, capabilities and end-user services, with cloud computing, the challenges faced in the healthcare industry with respect to managing the medical information, storing data, retrieving data or accessing could be eliminated. Here we store the patient information in the cloud by applying strong encryption mechanisms. The data from the cloud is accessed only by the authorized users and the information is completely kept confidential. 

Keywords—Cloud computing; Cloud system; Healthcare organizations; Electronic health records; Security and privacy; Body sensors 

I. INTRODUCTION 

Utilization of information technology in the sector of healthcare is significantly underutilized, particularly in areas of operational efficiency. Most healthcare researchers and institutions still rely on paper medical records, thus limiting collaboration and coordination between patients and physicians or doctors. As per the researchers studies and efforts in healthcare industry where they refer it must include cloud computing as a center piece for this transformation by National Institute of Standards and Technology (NIST) and the cloud computing can serve as a model which permits a set of configurable computing resources in sharing convenient and on-demand network access that are not usually provided in regular healthcare institutions. Cloud computing has both the broad network access and resource pooling which are intended to support big data sets from electronic healthcare records (EHR) where the features enable us to use computing resources by multiple consumers through different electronic devices such as mobile phones and tablets for providing more in-time access to critical medical data. Cloud computing system is a quantified based on the services that are provided and the ability to analyse and control all the resources and their usage in regard to the type of service provided in the areas such as storage and processing of data. Cloud computing also provides its clients with the desirable services which are supposed to be built on an infrastructure for facilitating the expected functions and which combine both hardware and software resources, these are also referred to physical layers and abstraction layers, where the physical layer includes various servers, storage and network components, and the abstraction layer consists of various software’s installed for carrying the services. Consumers or end-users also have their role in the cloud system where they do not required to manage the infrastructure itself as they don’t have the privilege of controlling applications by configuring their settings. In the same manner cloud infrastructure can also be provided for an organization and their consumers who may be related to a specific community or in a generalized manner may be related to the general public [1]. 

In healthcare organizations enormous amounts of data is collected and stored daily because the data is very important and vital for decision making and for delivering appropriate treatment process for patient and the healthcare organizations that intend to have EHRs towards exchange of data using cloud computing systems where patients’ data is stored or retrieved and further shared with other healthcare providers.

As the number of the healthcare organizations yield data is continuously increasing then eventually affect the storage capacity of the healthcare organizations where the data servers and other cause slowness in data retrieval as per the requirement
where the cloud computing is the solution for the—big data challenge [2] where the data providers provide unlimited storage resource and facilitates the process of sharing patients data between various healthcare organizations or for other use [3].

II. CLOUD COMPUTING AND HEALTHCARE ORGANIZATIONS

Due to vast increase in the average life expectancy that leads to faster population aging and also leads to increase in data records by which there exists growing demand for additional resources and a diverse medical care potential. Many innovative and cost-effective methods are required to contribute healthcare providers for finding more productive ways in addressing various profound global challenges that arise in day to day activities. Cloud computing must address practical solutions as in the new clinical information management system called —Health Value based Care Solution was developed in HIMSS17 in February 2017 by IBM and Active Health Management association where approximately 1,600 U.S. hospitals will receive performance bonuses in 2017 for hitting quality benchmarks, while over 1,300 will suffer penalties for missing those targets. As per the recent trends in industry IBM Watson Health is developing its first offerings to integrate the specialized capabilities of Watson Care Manager, Truven Health Analytics, Phytel, and Explorys. The new series of value-based cloud solutions are designed to help enable providers, health plans, and employers to improve the management of healthcare costs and quality by offering stakeholders innovative views of populations, potential risk factors and possible mitigation flags at an individual, group and population level. As the new IBM Watson Health Value-Based Care solutions will over time integrate patient-level data from a variety of sources, including electronic health records (EHR), hospital administrative and clinical databases, claims data and other sources to create a deeper basis for understanding and helping to predict future needs and behaviors. The first applications to be available later this year as part of the solution set includes:

- **Provider Performance Manager**: A profound quality management solution that enables healthcare providers to analyze and help project future performance threshold against specific value-based care benchmarks and incentives provided.
- **Engagement Manager**: A cognitive analytics solution is intended to track individual patient activity and engagement levels by incorporating hospital-specific process of care data and socio-demographic data to create a risk stratification of an entire patient population emerged.

- **Bundled Payments Forecasting and Management**: is the only expanded consulting service and set of new web-based tools that are designed to help healthcare providers by accurately forecasting future spending and identify cost centers that could trigger payment penalties and notifications.

- **Custom Analytics**: is an enterprise analytics offering that enables health plans and providers to embed the robust analytic content from Truven Health Analytics in their own technology environments without more specifications provided.

“We believe that the large scale movement to value-based models for care delivery and reimbursement means that healthcare providers and payers must now adopt different approaches to managing population health risk,” said Mike Boswood, General Manager of Value-Based Care, IBM Watson Health. “The value-based care solutions we are announcing today are designed to give hospitals, health plans, and self-insured employers the insights they need to understand how any one clinical or administrative decision can cascade throughout an organization and can potentially have dramatic impacts on both the cost and quality of care.”

III. SECURITY AND PRIVACY OF HEALTHCARE DATA WITH CLOUD COMPUTING

From electronic health records to mobile and web applications what are enabling doctors to improve health conditions and save lives where the doctors use these technologies to collect more information than ever before learning patients' health stories through the data they collect and these technologies and the data they contain connect and interact constantly by sending health information through increasingly complex systems with increasing risks and vulnerabilities. And no longer are doctors the only ones entrusted with intimate health information where the individuals managing the data storage which can access this information and thus have a responsibility to safeguard it all times.

Based on the sensitivity of health information in 1996 the U.S. government enacted the Health Information Portability and Accountability Act (HIPAA) and in 2003 the Health Information Technology for Economic and Clinical Health (HITECH) Act was formed where these laws tend to require entities that are responsible for sensitive health information to implement certain measures to
ensure privacy and security and to inform patients when the privacy and security of their information is compromised which merely happens.

Whenever any intended consumers migrate to cloud services for understanding these standards and requiring strict adherence to them is key to fulfilling an entity’s responsibilities and maintaining the trust of the patients who divulge intimate details for their health for providing a foundation for addressing related issues with cloud services.

The standards that are provided by HIPAA towards privacy and many specified standards contains certain health information which is known as the HIPAA Privacy Rule where these rules are applied to cover the entities by including healthcare providers data along with their plans and healthcare clearinghouses portfolio.

The active Privacy Rulesthat are provided by HIPAA under federal protection for available personal health information which is held by covered entities and gives patients with many rights that are related to the information act and at the same time Privacy Rule is also balanced suchthat it permits the disclosure of personal health information needed for patient care and other important purposes.

The HITECH Act required by the Secretary of HHS to expand the HIPAA Privacy and Security Rules which also increased the penalties for violations of HIPAA where the HHS Office for Civil Rights (OCR) has its jurisdiction only on the covered entities for privacy breaches and the HITECH Act with the HIPAA Privacy and Security Rules that are extended to apply with the Business Associates (BA) will be performing certain functions or activities that involve the use or disclosure of PHI on behalf of service providers to cover various entities and their services.

Other generalized security issues related to cloud computing environment are:

- **Data Breaches:** Cloud computing and services are relatively new and data breaches in all forms have existed for years. A study conducted by the Ponemon Institute entitled —Man In Cloud Attack‖ reports that over 50 percent of the IT and security professionals surveyed believed their organization’s security measures to protect data on cloud services are considerably low and based on scenarios a data breach had occurred and thereport concluded that overall data breaching was three times more likely to occur for businesses that utilize the cloud than those that don’t.

- **Hijacking of Accounts:** most of the attackers now have the ability to use the login information to remotely access sensitive data stored on the cloud and attackers can falsify and manipulate information through hijacked credentials which includes scripting bugs and reused passwords by allowing attackers to easily detect or steal credentials by performing phishing or keylogging or buffer overflow threats.

- **Insider Threat:** An attack from inside your organization may seem unlikely but the insider threat does exist where the employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer or accounts or financial forms and other sensitive information based on the study by Imperva “Inside Track on Insider Threat‖ found that an insider threat was the misuse of information through malicious intent or accidents or malware.

- **Malware Injection:** Malware injections are scripts or code embedded into cloud services that act as “valid instances” and run as SaaS on the cloud servers as the malicious code can be injected further into cloud services and viewed as part of the software or service which is running within the cloud servers themselves where an injection is executed and the cloud begins operating in tandem with it the attackers can eavesdrop or compromise the integrity of sensitive information and steal data that is specified by report submitted by the East Carolina University that profound to preview the threats of malware injections on cloud computing and states with malware injection attack that has become a major security concern in cloud computing systems.

- **Abuse of Cloud Services:** Due to expansion of cloud-based services which has made it possible for both small and enterprise-level organizations to host vast amounts of data easily the unprecedented storage capacity tends to allow both hackers and authorized users to easily host and spread malware or illegal software over digital properties that are often privileged by users who can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider.

- **Insecure APIs:** Application Programming Interfaces (API) give users the opportunity to customize their cloud experience and often APIs can be a threat to cloud security because of their very nature. But APIs give programmers the tools to build their programs to integrate their applications with other job-critical software to use.
Denial of Service (DoS)Attacks: DoS is also used as a smokescreen for other malicious activities to take down security appliances such as web application firewalls.

Insufficient Due Diligence: Many particular security gaps occur when an organization does not have a clear plan for its goals or resources and policies where the cloud diligence can pose a security risk or a threat when an organization migrates to the cloud quickly without properly anticipating that the services will not match customer's expectation.

IV. ENCRYPTION METHODOLOGIES AND CLOUD COMPUTING

The provision of cloud security is majorly built around various encryption methodologies that are mainly of four types: hashing encryption; symmetric cryptography; asymmetric cryptography and homomorphic. Where each method has several advantages and disadvantages based on their implementation or usage by cloud service providers who ensure whether the user data is not tampered with or compromised in any of its methods.

Hashing: This method uses a unique fixed length signature to encrypt every data set where the hash is created using a hash function or an algorithm and each hash is compared with other hash sets to verify uniqueness of the data set and on the same hand a small change in the data will result in the generation of a new hash value and the data owner will be alerted to any security breaches that may have occurred. This feature is not available in other kinds of encryption mechanisms as the hash encryption is irreversible which means that there are no decryption or de-hashing keys that can be used to reverse the process of hashing which makes hashing secure. One of such hashing algorithm that is commonly in use is Message Digest 5 (MD5).

Symmetric Encryption: Symmetric encryption uses same key for both encryption and decryption and the key is known as the "private key" and must be kept secure by the user if the data set is to remain secure and the key may be "user defined" or "system generated" one where the encryption operation maybe performed on a “stream of data” (encryption of one byte at a time) or a “block of data” (encryption of one block at a time) and some of the most commonly used symmetric algorithms are DES, AES, and Blowfish.

Asymmetric encryption: asymmetric encryption uses two different keys for encryption and decryption of a data set where the encrypting key is known as the “public key” and the decrypting key is known as the “private key” where the public key is freely available and the private key is available only to the person authorized to decrypt the message intended as the use of two keys is said to be the weakness of the system as considered by some of the researchers and some of such examples are RSA and Diffie-Hellman.

Homomorphic: these algorithms are making their appearances with the growing popularity of the Cloud era and a homomorphic algorithm is an encryption algorithm that allows the user to perform mathematical operations on the data set without decrypting the data or partially decrypting the data without loosing the bits of data.

V. POTENTIAL HEALTHCARE INDUSTRY BENEFITS FROM CLOUD COMPUTING

In the present era of information technology many industries benefit from the cloud it has been especially the case for the healthcare industry which is resulting in improved outcomes and some of the significant benefits to the industry are:

Data analytics: The exploitation of data by applying analytical methods such as statistics or predictive and quantitative models will provide better insights and achieve better outcomes, there is evidence of this: 94 percent of healthcare providers identified information explosion as the biggest factor anticipated to influence their organizations to a large extent over the next 5 years.

Security: Due to the regulatory compliance requirements for HIPAA, HITEC, PCI DSS and ISO 27001, the reluctance to adopt technology is starting being to be addressed and adopted by enchanting many of the security features required for data protection are addressed by the service providers therefore relieving the healthcare organizations from tedious and complex security frameworks.

Mobility: In cloud computing environment the main benefit is mobility whereby the cloud infrastructure is providing the backbone for medical personnel to access all sorts of information from any location and from a whole set of devices of distinct specifications.

Collaboration with patients: Patient records are now available anywhere, anytime for healthcare professionals which resuces the initial diagnosis and allows physicians to access critical historical
data and adjust their diagnosis based on informed decisions and some of such examples are:

- Physician Collaboration Solutions (PCS): These solutions facilitate remote consultations and care continuity which allows patients to be remotely visited and also offers video conferencing that allows physicians to visit patients in far out areas.

- Health Information Exchange (HIE): the healthcare information to be shared electronically across various organizations within a region or community or hospital system several cloud providers address this market by taking upon themselves the role of collecting and distributing medical information from and among multiple organizations.

- Electronic Medical Records (EMR): all the information pertaining to a specific patient or a segment of the population is recorded and stored by capturing and providing patient’s data at any time of the patient’s monitoring cycle which includes the complete medical records and its history.

VI. HOMOMORPHIC ENCRYPTION APPLIED TO CLOUD COMPUTING SECURITY ON HEALTHCARE DATA

When the data is transferred to the Cloud environment we use standard encryption methods to secure the operations and the storage of the data where the basic concept is to encrypt the data before send it to the Cloud provider where the last one needs to decrypt data at every operation for providing the private key to the server (Cloud provider) and needs to decrypt data before execute the calculations required, which might affect the confidentiality and privacy of data stored in the Cloud environment. In this paper we are proposing a novel application of a method to execute operations on encrypted data without decrypting them and all will provide the same results after calculations as if we have worked directly on the raw data.

Homomorphic Encryption systems will implement its operations on encrypted data without knowing the private key and the client is considered to be the only holder of the secret key, later when we decrypt the result of any operation as same as if we had carried out the calculation on the raw data. Definition [9]: An encryption is said to be homomorphic, if: from Enc(a) and Enc(b) it is possible to compute Enc(f (a, b)); where f can be: +, ×, ⊕and without using the private key as the Homomorphic encryption we distinguish according to the operations that allows to assess on raw data, the additive Homomorphic encryption (only additions of the raw data). Where: Ek is used for encryption of data, Dk is used for decryption of data where k is used for key.

\[ E_k(a) = \sum_k^n \text{OR} \quad E_k(a) \oplus E_k(b) = E_k(a+b) \]

The first property is called additive homomorphic encryption, and the second is multiplicative homomorphic encryption. An algorithm is fully homomorphic if both properties are satisfied simultaneously.

A. Multiplicative Homomorphic Encryption using RSA cryptosystem:

Let n=pq, where p and q are two prime numbers. By picking a and b such that both represents \( 1 \pmod{n} \), n and b are public while p,q and a are private.

A homomorphism: suppose X1 and X2 are plaintexts. Then ek(X₁)ek(X₂)=X₁X₂ mod n.

B. Additive Homomorphic Encryption in Paillier Cryptosystem.

The Homomorphism: Suppose X1 and X2 are plaintexts. The,

\[ C_k = (x_1, r_1) \oplus (x_2, r_2) = g^{x_1} r_1^k \cdot g^{x_2} r_2^k \mod n^2 \]

To perform operations such addition and multiplication on encrypted data stored in the cloud provider, the client must have two different key generators (one for RSA and one for Paillier) and we present in what follows the El Gamal cryptosystems that is basically a multiplicative homomorphic cryptosystem but by modifying coding mode we can make it additive.
VII. CONCLUSION

Cloud computing system is considered to be a measured service that comprises of the ability to automatically control and optimize various resources that are considered to be regarded to the type of service provided. Healthcare organizations need innovative and cost-effective methods to assist healthcare providers and tend to find more productive ways to address growing numbers of patients and their data is considered to be very vital and the Electronic Health records (EHR) pattern. The security is based on Homomorphic Encryption which is a new concept of implementing security that enables to provide the results of calculations on encrypted data without knowing of the raw EHR entries on which the calculation was carried out respecting the confidentiality of data. In our proposed future work we are going to analyse the behaviour of Homomorphic Encryption cryptosystems by comparing the length of the public key and the time of considerable treatment using encrypted messages and their various forms.

REFERENCES
