ISSN 2278-3091
Volume 8, No.3, May - June 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse97832019.pdf
https://doi.org/10.30534/ijatcse/2019/97832019

A Survey on implementing privacy in Healthcare: An Indian Perspective

Navid Kagalwalla[1], Tanvi Garg[1], Prathamesh Churi[2], Ambika Pawar[3]
[1]Computer Engineering Department, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India, navidkagalwalla@hotmail.com, garg9925@gmail.com
[2] Ph.D. Research Scholar, Computer Science and Information Technology Department, Symbiosis International (Deemed University), Pune, India, prathamesh.churi@gmail.com
[3] Associate Professor, Computer Science and Information Technology Department, Symbiosis International (Deemed University), Pune, India, ambikap@sitpune.edu.in

ABSTRACT

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."- Marlon Brando Privacy in Healthcare is the practice of maintaining the security and confidentiality of patient records. With the advent of new technologies in healthcare such as EHRs, pharmacogenomics and genome sequencing, etc. the focus on securing the patient's data and identity hasn't been given as much importance. The issues in healthcare privacy stem from a lack of infrastructure, complacency, budget constraints, and politics. The paper explores the issues which plague the healthcare industry in its fight to secure patient data from potential exploitation. Hackers can use this easily attainable healthcare data for profit and identity stealing which is a major concern. In this paper, we have reviewed multiple papers and specified their description along with their inferences, future research, and research gaps. The paper has a strong base of 36 research papers and review papers which are mentioned and cited. Finally, this paper presents solutions on how to mitigate the various issues present to make healthcare data secure and safe from exploitation. The paper limits the study of proposing privacy models in India as a country.

Key words: Privacy, Healthcare, Big data, Cloud, Security, HER.

1. INTRODUCTION

'Privacy' as defined by Cambridge's dictionary is "Someone's right to keep their personal matters and relationships secret". The Universal Declaration of Human Rights also secures the right to privacy by stating, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Privacy is defined as an action where the data is kept hidden from either an anonymous user, server to avoid the use of malpractice of the data. Privacy is a fundamental human right. It is key to freedom of thought and speech. Privacy is the right of people to make confident decisions regarding their own lives independent of public scrutiny. A security and privacy concern of any type of data is a major issue in today's technology-driven world. Information privacy is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to. With the rapid pace of technological innovation, information privacy is becoming more important, as more data is collected and exchanged.

Health IT is often considered a silent partner in healthcare – not seen by patients, but an essential part of the system [21] [22] [23]. Breakthroughs in technology related to information gathering, research, treatments, and communications have given medical providers fresh ways to practice medicine and modernized healthcare. Technology has improved healthcare by making solutions to various ailments easily available to the public with the help of the Internet. Healthcare facilities can now reach people using social media. Improved facilities lead to better treatment and less suffering as well as improved worker efficiency. Further, doctors are easier to reach and online databases can accurately predict medical trends.

Tremendous technological advancements have emerged over the last ten years. The EHR (Electronic Health Record) [24] [25] is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make data available instantly and securely to authorized users. EHR has already created big strides in the centralization and efficiency of patient information; it can also be used as a data and population health tool for the future.

Sensors and Wearable technology are a simple way to collect data which is the aim of healthcare. Sensors and wearable technology could be as simple as an alert sent to a care provider when a patient falls down or a bandage that can detect skin pH levels to tell if a cut is getting infected [26] [27] [28] [29] [30]. Real-time locating services in healthcare are another emerging data monitoring tool. It helps hospitals focus on efficiency and instantly identify problem areas. Hospitals can implement tracking systems for instruments, devices, and even clinical staff. Pharmacogenomics and genome sequencing is a type of personalized medicine in which treatments are tailored according to individuals and diseases are anticipated in advance. This leads to healthcare efficiency and diagnostic accuracy.

These ground-breaking technological breakthroughs in

healthcare however, come at a cost – privacy and security of the patient and the data are undermined. Healthcare data, location of a patient or staffer, personally identifiable information is not focused on and kept secure in these new technologies.

Privacy issues in healthcare range from being common to the full world, to be specific to each country and it's demographic. The general problems with healthcare in terms of privacy are the insecure storage of personally identifiable information. Healthcare data of patients should be kept private and only after the consent of the patient should the data be made available for research or other purposes but personal information should never be shared. Healthcare data should not be shared with third parties. Tracking of patients without their consent should be prohibited. Database administrators should be given a multifactor authentication scheme and they should not be allowed to share data without permission. Further, data stored in databases should be anonymous, only being linked by a key to each patient to preserve anonymity. Adequate security measures such as firewalls, multifactor authentication, role-based access control, secure remote access control; encryption, etc. should be taken to prevent intrusions such as MITM, data leakage, viruses, DOS, etc.

Privacy issues in healthcare-specific to India are due to prevalent complacency, culture, politics, budget limitations, huge population and the infrastructure present. Due to these factors, data security takes a backseat allowing for easy access to confidential information [31][32][33]

Often healthcare data of one individual is stored on another person's name which leads to inconsistency in data. Also, multiple people having the same name leads to confusion. It is very hard to keep track who is the real patient behind the data and who is the author who entered the data. Issues related to infrastructure also hinder the privacy and security of healthcare data. There is no common healthcare system/database established to store healthcare data of every citizen of India. The lack of good architecture not only affects the security and privacy of healthcare data but also affects the level of treatment and care given at various healthcare centers.

Hackers target healthcare information since their major objective is to misuse and exploit personal information which is a lucrative business. Comprehensive medical records can sell on the black market for huge sums since the data includes names, birthdates, insurance policy numbers, aadhar card numbers, billing information, and diagnosis. This data can be used to create fake IDs to buy drugs or used to file fake insurance claims. Thus securing healthcare data is of utmost importance.

Healthcare data is highly private. The medical and psychological conditions of patients cannot be made public since it may affect insurance coverage or employment. Doctor-patient confidentiality is another way by which privacy can be maintained. Protecting the patient's integrity and dignity and ensuring the patient's comfort to reveal accurate information to receive the correct treatment can only be got by having robust security and privacy measures in place.

The proposed literature survey examines the recent privacy measures implemented in the healthcare industry. It identifies the need for security and privacy in healthcare and the various ways in which these privacy measures can be implemented. The paper reviews the previous work done by other papers on privacy in healthcare. It describes the methodology and analyzes the ways in which privacy can be maintained. It discusses the inferences and research gaps involved with each paper reviewed. Further, this paper explores the challenges faced in keeping healthcare information private and secure. Challenges in securing healthcare data are diverse and range from a lack of infrastructure and funding to data breach and trust issues with third parties. Keeping in mind these challenges the paper comes up with solutions to tackle these issues and help make confidential healthcare and PII secure. The solutions presented can only be successfully implemented if all the parties involved viz. government, healthcare institutions, healthcare specialists work together to make healthcare data secure.

2. RESEARCH ON PRIVACY IN HEALTHCARE

2.1 Research in 2015

Citation and Type of paper	**2015 papers on privacy in healthcare**	
	Description	***Inferences and Future Research***
[1] Research paper	• This paper is about the accessing and transferring of information over an encrypted relational database • A private key generator (PKG) is used to generated to decrypt the message • The medical details are entered in the branching algorithm and on that basis the patient	• The evaluation and execution of the proposal are to be done practically and then further decisions can be taken.

Citation and Type of paper	2015 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	receives medication • Proposes layered encryption to support the queries. For such as queries database doesn't have to be decrypted to be accessed.	
[2] Review Paper	• The active privacy bundles(APBs) that group[sensitive data, metadata, virtual machine(VM)] combined with trusted third parties(TTP) to maintain trust level. • The first high-level phase of an APB lifecycle is APB Creation in which an APB is constructed, VM computes the hash value and encrypts the APB. The decryption key is given to the TTP • The second level is the APB enabling to give the data to the virtual host(VH). There are two stages in this: o **Verification status:** where you check if the VH is trusted or not with a minimum trust level value by the metadata and checking the integrity level of the APB by computing the hash value from the decryption key and checking with the original hash o **APB enforcement:** in this, if the trust level is not met by the VH then VM destroys full or partial data, display full or partial data.	• Improving APB-TTP to include an automatic negotiation of privacy policies • Applying APB-MA for protecting patients' privacy in electronic prescription transfer (EPT)
[3] Research Paper	• The proposed architecture in this is the publish/subscribe(Pub/Sub) architecture to share the data securely • This architecture is moderated by the web service uses the RabbitMQ which communicates via advanced messaging and follows a neutral protocol. It is durable, persistent and scalable and an open-source. • The web service has to authorize and control access and this is done by role-based access control(RBAC) that groups the users based on their activity • Web service also must provide the right level of expressiveness and is achieved by disaggregation of data through tags automatically created by the web service	• Since this proposed architecture uses self-defined exchange format, in future it should be changed to predefined exchange format such as(HL7, SDMX-HD) • The connection between the host and web service to be encrypted • Future research is to go beyond these standard access control and authentication techniques and come up with custom privacy model for public health requirements.

Citation and Type of paper	2015 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	• Data consistency in the required format is ensured with CIEL/MVP by ensuring that the tags and information is part of the metadata • Connector resides in the host machine which is responsible for the exchange of information between the web service and hosts.	

2.2. Research in 2016

Citation and Type of paper	2016 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
[4], Research Paper	It uses Global Patient Identification Technique • Key(GPIK) is generated for each patient record using a mobile number, name, and sex. • Name is converted to NAME VALUE by removing vowels from the name and then encrypted. • Mobile number is encrypted and then concatenated before NAME VALUE. • This key(GPIK) along with the GEOCODE and BIRTHYEAR of the patient is stored in the recordset.	• Patients can use multiple mobile phones or change mobile numbers which will impact the mining results. • Assumes all patients have mobile numbers.
[5], Research Paper	It uses Multi Authority Attribute-Based Encryption. • Provides enhanced encryption in comparison to Cipher Policy Attribute-Based Encryption. • Provides fine-grained and patient-centric control. • Enhances system scalability and resistance to outsider attacks like Man-in-middle attack, denial of service(DOS). • The administrator can only access the patient healthcare data by patient consent or by doctor consent thus ensuring security.	• Third-party sources can still access data. • Data administrator can steal data.
[6], Research Paper	It uses Cloud-Based EHR with Key-Control Scheme • **Pairing -** The patient chooses to give the authority to one physician to access his/her medical record on the cloud at any time. Done by pairing the secret keys of both into the key access management scheme. • **Assertion –**The patient must actively log into his patient account before the physician can access the healthcare record. Rural practitioner or physician must be paired with the patient to access or write a record. • **Cross-authority access & privacy mechanism –** In times of emergency when a patient and physician are not paired, the physician accesses that patient's health history by	• The proposed scheme is scalable. • As the number of records increases the time to access it linearly increases.

Citation and Type of paper	2016 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	getting consent from the patient's family. Privacy-preserving algorithms based on ASM Privacy Homomorphism are used. • **Write record operation –** Includes patient verification, assertion to a physician, generates a key set (public key(Pk) and private key(Sk)), session id. Encrypted record is then sent to cloud backend which decrypts the record with Sk, encrypts record with a new set of keys and stores the record with the session id. Stores the session id and a new set of keys in another table. • **Read record operation –** Includes patient verification, assertion to a physician, physician verification. Cloud backend gets the read request. It collects the records with session ids corresponding to the patient, decrypts the record using private key stored in the cloud key table and then encrypts the record such that it can be decrypted using physicians secret key. • Elgamal algorithm for text encryption used. Although ID-based encryption, Attributes based Encryption or Predicate based Encryption can also be used.	
[7], Review Paper	It identifies three modalities of security for healthcare: • **Administrative** 1. Chief Information Security Officer 2. Risk Analysis and Management 3. Continued System security evaluation 4. Disaster Recovery Planning • **Physical** 1. Physical Access Protocols 2. Workstation Security 3. RFID • **Technical** 1. Entity authentication 2. Data encryption 3. Firewalls 4. Virus checking 5. Access control 6. Audit trails	• The summary showed that Technical safeguards were used the most, followed by Administrative and lastly Physical. • Facility-specific security techniques, in addition to the inceptive cost, and the implementation and maintenance costs of these safety measures must be discerned. • It is very hard to determine which program or technique performs the best in regards to preventing data breaches in healthcare.

2.3. Research in 2017

Citation and Type of paper	2017 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
[8], Review Paper	Technologies used include • **Authentication –** Secure Sockets Layer or Transport Layer Security to authenticate the server using a mutually trusted certification authority. Bull Eye algorithm can be used for	• Paper investigated the security and confidentiality issues in big data. • Increased complexity and limitations make models more difficult to interpret and lower

Citation and Type of paper	2017 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	monitoring all sensitive information in 360°. This algorithm makes sure that the data is secure and there is a distinction between original and replicated data. The user must be authorized to be able to read or modify this confidential data. • **Encryption –** It must be ensured that the encryption scheme is reliable, scalable and easy to use by both patients and healthcare professionals. The number of keys held by each party should be minimized. • **Data Masking** –Sensitive data elements are replaced by unidentifiable values. It uses a strategy of de-identifying the data sets or masking personal identifiers such as name, social security number and suppressing or generalizing quasi-identifiers like date-of-birth and zip-codes • **Access Control** – Users can perform only those activities for which they have been granted permission such as data access and modification, job submission, etc. This uses authorization protocols such as Role-Based Access Control and Attribute-Based Access Control for EHR.	their efficiency. • Every algorithm, encryption, anonymity technique present has certain disadvantages. Thus no technique is perfect and each situation may prefer a different technique. • Future research will focus more on achieving effective solutions to the scalability problem of big data privacy and security in the era of healthcare. Different test cases should be envisioned which will help in implementing a privacy model which is efficient, reliable and scalable.
[9], Review Paper	The Paper uses IOT based Healthcare System using Cloud Computing. • **Data Governance –** The big data scheme used should be scalable, only sensitive and confidential healthcare data should be stored and classification of data which is no longer useful should be made efficiently. • **Heterogeneity** –Capability of dealing with diverse figures imminent at dissimilar velocities. • **Real-Time Security Analytics** – Forecasting risk sources. In IoT scenarios of healthcare, applying security in resource controlled network architecture is important. • **Disaster Recovery** – Data should be stored in the cloud using database management systems which can tolerate faults and easily recover the data in times of disasters. • **Analytics for Privacy Preservation** –Before the IOT devices send the sensitive healthcare data to the cloud, it should be processed, studied and analyzed in an interim decentralized approach.	• Paper highlighted the most probable security and confidentiality problems of big data in healthcare. • IoT based healthcare system remotely gather a large number of data which is needed to be stored in the cloud infrastructure so big data is the optimum solution for storing such a big amount of data with proper structures and relations.
[10], Review Paper	• The records of the patients should be stored as in the form of EHR as it is more effective and the cloud-based system requires less cost. • For parties to access the data in HER, there is a third party involved who ensures with whom the data is shared and the level of abstraction	• Most of the suggested models fail to address the security and privacy requirements. • The hybrid cloud-based HER system design was proposed but has not been tested.

Citation and Type of paper	2017 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	in sharing. • The CIA(Confidentiality, Integrity, and Accountability) triad should be mandatorily satisfied. • To access the protected data, four different access control methods can be used: o **Discretionary Access Control (DAC):** subjects inherit and transfer rights to each other unless specified otherwise. o **Mandatory Access Control (MAC):** the access is managed by a central authority. o **Role-Based Access Control (RBAC):** here the user creates roles based on their function and the access is granted to the roles. The steps followed are role assignment, role authorization, and transaction authorization respectively. This model guarantees data abstraction and separation of duty. o **Attribute-Based Access Control (ABAC):** instead of assigning roles to the requests this assigns attributes and are evaluated based on these to get access. Since every request will be given a different attribute there will be no redundancy.	
[11], Review Paper	• The use of Big Data in healthcare industry becomes important to keep track of the patients, their records. • The problems faced in this are the security problems, the secure connection of the cloud and IoT, abstraction between users and servers, etc. • The architecture discussed here is the Meta Cloud (MC) architecture. Here sensor medical devices are fixed with the human body to collect clinical measures of the patient. The working of this architecture is: o Collects data from various cloud generators for processing purpose o Used to provide optimal solutions o Provides knowledge to stakeholders • Big data is not possible to encrypt as a whole so it encrypts the path and gets the cryptographic virtual mapping of data. • The proposed system uses a key management security mechanism to protect big data in the industry.	Issues with the security system here are : • Even though there is encryption, this technique is not very trustworthy as it ensures confidentiality, not integrity • Since the data path is encrypted and not the data, this architecture fails. • Data lineage(path of data) makes the location of data easy but is very time-consuming.
[12], Review Paper	The paper uses Big Data to implement EHRs. • **Instantaneous Security Analytics –** Examining the possible security and privacy	• Paper investigated the security and confidentiality issues in big data. • Paper discussed recent progress in

Citation and Type of paper	2017 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	threats and at the same time computing the threat sources instantaneously to take protective procedures. • **Privacy Maintaining Analytics –** The incursion of patients privacy is on the rise. To curb this, privacy-maintaining encryption patterns that keep the data anonymous as well as taking consent from patients for using their data. Innovative privacy protection laws must also be implemented to keep up with times. • **Data Leakage –** **1. Organized Access –** The privilege of entry through consent remains the most general technological methods used to have security against the illicit right to use collected data. **2. Multi-Factor Authentification –** Two or three authentication factors are used which are generally passwords, credit card and fingerprints. 3. **Data Leakage Prevention** – Data packets are assessed locally and data' s movement is controlled within departments from its internal network, with the execution of protocols that are based on data locality and file organization. • **Data Privacy –** Fears to confidentiality and privacy stem from the negligent revelation of an individual's data, the mistreatment of the data and the fact that resultant data might be inexplicit or fabricated. • **Data Sharing –** The conventional approach of any cloud storage is that they store plain text or encrypted data inactively. The data stored normally is well-thought-out as " dead" because there is no involvement of any calculation. Big data allows the exchange of this data which may contain confidential information stored as plain text.	the field of data storage, privacy, sharing, patient records, healthcare-related databases, and real-time data protection and security.

2.4. Research in 2018

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
[13], Review Paper	Technologies used to ensure that big healthcare data is confidential and secure are: • **Authentication –** Plays an indispensable role in an organization; securing access to networks, protecting the identities of users and ensuring that the user is really who he is pretending to be. Endpoint authentication is used to prevent MITM attacks. Hashing techniques like SHA-256 can be used to	• Paper investigated the confidentiality and security issues in big data. The potential opportunities offered for big data in the healthcare arena are unlimited but there are several hindrances that impede its true potential like technical and confidentiality issues.

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	achieve authentication. • **Encryption –** It protects and maintains ownership of data throughout its lifecycle—from the data center to the endpoint and into the cloud. Data which is encrypted cannot be breached using packet sniffing and theft of storage devices. • **Data Masking** – Replaces sensitive data elements with unidentifiable values. It uses a strategy of de-identifying data sets or masking personal identifiers. Examples are k-anonymity and p-sensitive anonymity. • **Access Control –** Once authenticated, the users can enter an information system but their access will still be governed by an access control policy. This policy is governed by the patient or by a reliant third party. • **Monitoring and Auditing –** Security monitoring is necessary to catch intrusions in the network. Audit means recording user activities of the healthcare system in chronological order, such as maintaining a log of every access to and modification of data.	• The quality of data should not be affected by privacy-preserving algorithms but at the same time, data must be secure. The problem of reconciling security and privacy models by simulating diverse approaches to ultimately support decision making and planning strategies is the need of the hour.
[14], Research Paper	The proposed system includes the following steps: • **Input Selection –** The patient dataset which holds attributes like name, age, gender, symptoms, etc. is taken as input. • **Data Encryption and Anonymization –** Collected data must be encrypted. Triple Data Encryption Standard (Triple DES) is used. After encryption, the data is stored in the big data. Anonymization is used for hiding the receiver's information. • **Big Data Storage –** Includes directly attached storage pools, scale-out or clustered network-attached storage. Storage infrastructure is linked to computer server nodes which allow swift processing and retrieval of large measures of data. • **Data Sharing –** Conditional sharing method exists to prevent the same dataset from being changed by two people simultaneously. It uses A3DES algorithm for data sharing as an encryption method. A3DES Algorithm Steps are as follows – 1. Encryption and anonymization are done on the input selected from the dataset. 2. 3DES is used for Data encryption. 3. PSO optimization algorithm is employed for the selection of string	The paper proposed an approach to lessen the security issue in the big healthcare data storage. • A3DES (Anonymization and Triple DES) offers better security as it encrypts data thrice. • A3DES algorithm decrypts the data 3 times, thus it is more secure. • Noise anonymization technique is modified. Thus more security power and accuracy is added to the big data storage. The proposed system is superior and well secured than all the other existing ones.

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	position. 4. Conditional sharing is now done if the condition is satisfied. Else, selected data is aborted.	
[15], Research Paper	The important components in the proposed model are: • **Identity –** Personally Identifiable Information (PII) should be protected from unauthorized access. • **Privacy** – It is the ability to keep PII safe from unauthorized access. • **Anonymity** – E-health records should not be traced back to a patient, rather to a group of patients. It allows the user to utilize or access a resource or a facility without revealing any PII. • **Unlinkability –** The unsanctioned and unauthorized organization or person should not be able to link the healthcare data to a single patient. • **Anonymous Credentials –** The blind signatures based on RSA is used to utilize various cloud services anonymously. The methodology and execution of the proposed scheme are: • **Authentication Scheme** – Various steps involved are: 1. Registration and each Users Adaptive privacy policy creation 2. Obtaining an Access Ticket 3. Using this Access Ticket to gain access to various resources. • **Scheme Components –** Various components involved are: 1. User 2. Cloud Service Provider 3. E-Health Registration Ticket Manager 4. E-Health Service Manager • **Authentication Protocol –**The patient cannot be identified using this scheme. Thus the e-Health provider will only receive a request for the healthcare data without any PII being transferred. This scheme can also be validated using the Scyther tool for automatic validation and verification. In this scheme, the two-session keys strengthen the environment for exchange while the access ticket is created by the RTM and while the service is used with the Service Manager(SM).	• Using Cloud Computing to provide effective and low-cost healthcare services to tackle the privacy issues of healthcare information. • Patients get access using anonymous credentials without revealing personally identifiable information. • The system achieves reliable efficiency in aspects of computations and space complexity with reasonable overhead due to the communication paradigms. • Future work according to this paper will include preserving the confidentiality of a patient by IP spoofing. This helps keep the location of the patient anonymous.
[16], Review Paper	The paper deals with the following: • Security and privacy problem of healthcare data have both a technical and moral aspect.	• Authentication is required for the following purposes: 1. Prevent Impersonation

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	• Encryption is useful in securing data and relies on authentication. • Logging in to a database can be a serious authentication problem because others could impersonate the user which may lead to information leakage. • Three ways for authentication login are: 1. What you know – Authenticates based on a password or a secret question. 2. What you have – Authenticates based on the something the user has, like a device. A one-time password sent to the device may be used. 3. What you are – Authenticates based on biometrics. • Trust between a patient and the data user (researcher) is fundamental. • It is important to outline the measures which will be taken in case of leakage or loss of authentication key.	2. Demonstrate intent 3. If the user forgets the key, he/she should be able to change it. 4. User-friendly • Currently, the most viable option is the two-factor authentication combining a password and a one-time password. • Biometric authentication is likely to be useful in the future. • In addition, Ethical committees should be set up to review the authentication system.
[17], Research Paper	• The wireless sensor networks (WSNs) are classified into e-healthcare, m-healthcare, remote healthcare, etc. and the use of internet services makes privacy a vulnerable topic and is looked after by secret sharing and multipath routing • The data is split into N components. These components are transferred to n servers. This is done with the help of multipath routing. • Multipath routing is a maximum number of disjoint paths from the source to the destination. • Hash functions are computed for each component and send to the servers. These hash functions are used to retrieve and reconstruct the data • Security enrichment is done by Shamir secret splitting. This involves: 1. The secret is distributed such that the recombination makes sense. 2. Provides robust control and removes single point sensitivity 3. The given function is split keeping the conditions in mind 4. These smaller functions are given to n servers with the help of multipath routing 5. A hash function is calculated such that the functions can be sent to n servers without getting lost • This paper proposes an architecture where the message is split, a hash function is computed at the receiver side, apply	• Privacy is secured with hashing where the actual message is split and sent to different servers. • The results of this scheme provide superior performance compared with plain text transmission in terms of privacy and security preservation.

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	multipath routing on shares, check whether the hash received and hash computed are same or not. If they are same then accept or else reject.	
[18], Review Paper	• This paper introduces a Boolean model that reveals the connection in privacy, security, and big data. This helps with the understanding of privacy and security at three levels in the big data paradigm: fundamental, interactional and integrated. 1. Fundamental level: at this level the privacy, security and big data 2. Interactional level: here relationships between two of the elements are seen. For example, privacy and security, security and big data and big data and privacy. 3. Integrated level: all the three are seen together, i.e. privacy and security in big data • Research and development of big data-driven privacy and security. This is done by using big volume-driven, big velocity-driven, big variety-driven, or big accuracy-driven privacy and security in the big data age. • This research has three practical implications for confidentiality and security in the big data paradigm: 1. The statistical analysis of big data-driven privacy and security can facilitate the researcher to carry out research because they understand that big data-driven confidentiality takes about 2% of all the research. 2. The proposed cutting edge privacy and security techniques might be of interest to organizations to invest in research and development on "formal methods and theory of security" and "human and societal aspects of security and privacy" because they are the two implausible research areas in big data. 3. Practitioners and researchers might use the Boolean model and classification of big data in terms of privacy and security to come up with a new information system for obtaining confidentiality in the big data age.	• Talks about analysis and classification of security and privacy • The future scope is to investigate each of the proposed classifications individually in terms of technology, governance and policy development.
[19], Research Paper	• Distributed learning (DL) is proposed in this paper as it preserves the privacy of the patients' and maintains data ownership predicting models.	• This technology allowed the supervisors to detect the problem without accessing the data. • The future work includes the

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	• This architecture involves site and master. The sites stores the data of the patients and only cumulative statistics are exchanged with the central server. The master computes parameters sent to a single site and finds the convergence criteria. • The privacy in the above architecture is defined by two tools Chi-Square test and linear and logistic regression model. • Chi-Square test access the patient data and calculates the occurrences in each interval value and if it's available in the statistical analysis tool after calculating using the Chi-Square test then it can be used top-value statistic parameter. • Another method is Distributed Chi-Square test and linear and logistics models implementation where the patient data is inaccessible and never leaves the site. This is done by exchanging message between the master and site iteration by iteration. Where site calculates one part and sends to the master and the master receives the data, processes it and replies back.	application of these methods on various test cases to see if they can provide an efficient and successful output.
[20], Research Paper	• The proposed system has two key components: functional, that deals with system potential for healthcare data analytics and management and non-functional that deals with security, confidentiality, consent, scalability and performance capabilities. • The model has three parts: infrastructure cloud that provides compute and storage resources, health cloud platform services that provide secure generic services (DevOps), high availability and disaster recovery service, federated identity management service, analytics platform and some health care specific services, and customized client services which make the client interaction easy. • The system and user-level view of architecture are overall from the system from the perspective of the user. Caches are used to store data and algorithms are depending on how frequently data is getting modified. This system also uses external databases. • **Threat model:** private and sensitive healthcare and life sciences(HCLs) should be reliable and trusted. For these two models are described Honest-But-Curious Adversaries which say that a protocol should be defined and everyone should follow it. If this protocol is secure the data is secured. The second model is Malicious Adversaries that say	• The proposed cloud-based system offers enhanced security and privacy. • This system is used in Drug Repositioning, Drug Effect Signal Detection from Real World Evidence Data.

Citation and Type of paper	2018 papers on privacy in healthcare	
	Description	***Inferences and Future Research***
	arbitrary values should be defined for private inputs or abort the protocol prematurely. • **Security:** security involves that of the data, system, and users. In data security, the data is encrypted at a level and verified when access is requested therefore HMACs is recommended instead of digital signatures. Verification ensures integrity and authenticity, scanning of data for malware, verification of the level of privacy and consent of the patient. The system is secured by authorizing access by digital signatures. • **Privacy:** blockchain can keep track of privacy degrees of data records • **Regulatory compliance:** this makes sure that the privacy requirements are met and no rule is violated • **Auditability:** regulatory requirements and security forensic analysis make audits mandatory.	

3. CHALLENGES OF PRIVACY OF HEALTHCARE DATA: INDIAN PERSPECTIVE

3.1. Data Storage and Management [1] [3] [6] [11] [15]

With an increasing number of patients, it is important for the EHRs to update themselves. The huge population of India presents problems since different dialects are used and thus converting EHR from one dialect to another can prove to be a cumbersome task. Also, EHR can only be inclusive for the whole country if it involves the active participation of the full country which again is hard due to India's huge population. The information involves continuous refreshing and expanding and thus the framework ought to be forward-thinking to store all the recent data. In cloud and IOTs it is said that the data should be synchronized and accessible without interruptions, delays, and jitters. Data storage and management is a major issue in this industry. Data management additionally includes that design is going to be best to store the info, centralized or distributed, looking on the confidentiality and demand of data.

Another issue is the threat to the doctor-patient relationship. Patients may not have confidence in the party which secures the data and may thus hesitate to disclose their PII and accurate health data which can lead to discrepancies. If accurate healthcare data is not disclosed it can lead to future complications when doctors have to give medication again. Security is a key right and if the data imparted to the data administrator is made public, it affects the doctor-patient relationship, hence causing a stir. This has been mentioned in the paper "Improving Privacy in Healthcare Service by Using Cloud Assisted Technologies". Hence, this is another viewpoint remembered while structuring the design for a secure healthcare system.

3.2. Cyber Attacks [17] [18]

The various Cyber-attacks like Denial of Service(DOS) attack and Distributed Denial of Service (DDOS) attack affect the data of the patient and make it very vulnerable. The DOS and DDOS attacks are those in which the exploiter tries to exhaust the resources available to the network by sending extra unnecessary packets. These are a threat to the patient data as it makes the patient data vulnerable to the attacker but the healthcare providers find it difficult to access the network for various activities like accessing the records, sending and receiving emails, or any sort of information using the network.

3.3. Data Sharing [3]

Data exchange is a major concern for healthcare since questions like who should access the data, how much data should be visible to the client, how much abstraction of data should be done at each level, whether the data is secure or not, etc. that make data sharing vulnerably tough. Therefore, these problems have to be dealt with while brainstorming for a secure solution to the above problems.

3.4. Trust in the third party [2][5]

While some software in the healthcare industry uses a third party that controls the information and oversees who gets to view the information and how much information can

be made visible to the client. Cloud storage can be vulnerable while storing a large number of patient records since it is in the hands of a third party. The issue with this system of healthcare is whether the third party can be trusted and the information used isn't misused by the third party. There is a probability that this outsider isn't unbiased and favors a couple of enterprises and may prompt information rupturing. The usage of external party questions the confidentiality and integrity of the system questioning its usage and making it an important issue to be dealt with during the building of the architecture that is more reliable.

3.5. Infrastructure [18]

In the healthcare industry, it is very important to have a secure infrastructure. The infrastructure required to make the privacy of healthcare data a reality requires substantial investment and backing from the government. The government should be committed to making changes and should be ready to provide funding to completely overhaul the healthcare system to make it more patient-centric and privacy-oriented. A proper structure and protocol should be present on the ground at each medical center, be it urban or rural to make the data secure and safe from tampering. The infrastructure of the system should be safe and yet easy in every aspect, that is,

Interoperability: exchange of data should be secure and under control

Security: no party involved should have full access to the data

Regulations: privacy of no patient should be violated

Availability: the data should be available at the required date and time of whichever person under full authorization

Integration: there should be layered and step-by-step access to information using any particular architecture.

Therefore, infrastructure is a very sensitive part and is a major issue in most of the healthcare systems.

3.6. Absence of Privacy Policy by the Constitution [20]

The essential test of security in medicinal services in India is the nonattendance of an administration arrangement that ensures the protection of the patients. The absence of said strategy and infrastructure that keeps the protection of patient's information secure legitimately is a cause of worry. Numerous nations as of now have such arrangements, for instance, the HIPAA demonstration in the US. This arrangement sets up the standard for EHR exchanges and sets guidelines for the wellbeing associations to get to the EHR and to stay in compliance with protection guidelines. The nearness of this approach makes it simpler for the wellbeing associations to utilize the EHRs and keep up the security under lawful terms and along these lines. India, where protection is a delicate issue and the data can without much of a stretch be gotten to except if a solid data framework is utilized, requires an arrangement to set standard procedures for each social insurance association.

3.7. Data Breaching [10]

A data breach is when a sensitive, protected and confidential data is stolen, copied, transmitted, viewed or used by an individual unauthorized to do so. Some healthcare organizations have integrated distributed heterogeneous systems that share the patient data with healthcare, pharmaceutical companies, researchers, insurance providers and all the parties involved in the system. This is illicit exchanging of individual data to assist the organization. Another way is to get unauthorized access to data by the user. For example, using cloud-based access control in EHRs, are very vulnerable and can provide all details once accessed and therefore, these issues are hence used by some clients to get personal information.

3.8. Culture

The culture prevalent also affects healthcare disclosure in India. In many cultures, the disclosure of sensitive personal healthcare data is looked down upon. This leads to discrepancies in the healthcare data recorded as well as a decrease in the level of treatment meted out. Research and statistics of treatment given then don't match the records due to inaccurate reporting of data.

3.9. Prevalent Complacency

Complacency is widespread in India. Bureaucrats are never shy of giving promises but do absolutely nothing to fulfill them. The work, planning, cooperation and communication required amongst multiple departments to make privacy and security of healthcare in India a success is gargantuan. However, due to slackness, the probability of a privacy model actually being implemented in India is poor. Bureaucrats should be ready to do good work within stipulated deadlines to make the privacy of patients and data a reality in the near future.

3.10. Increased Instances of Hacking [4]

Hacking is increasing at a shocking rate. The main cause of breaches in healthcare data is due to hackers targeting digital medical files. Hackers change the methodology of attack used since healthcare data, rich in PII is valuable. Thus implementing a sound privacy model which can handle various kinds of attacks is a challenge.

3.11. Accountability [4]

In a National Health Data Warehouse [34] if a patient's sensitive and private data leaks, the authority responsible should be clearly specified. Who would be liable for a defamation suit should be specified. It is not possible for doctors, researchers, and healthcare providers to guarantee full privacy due to unknown circumstances.

3.12. Cost

The cost required to implement a privacy model is substantial and requires funding from the government and individuals. To make the privacy model a success, it involves the work of specialists in the field of privacy and in the field of healthcare. Budget constraints may lead to an ineffective model getting implemented which won't be secure and safe from attacks.

4. PROPOSED SOLUTION OF IMPLEMENTING PRIVACY MODELS

Sr. No.	***Challenges***	***Proposed Solution of Privacy Methods*** ***Proposed Solution***
1.	Data storage and management	While India's population is showing a decline, the rate at which the population is declining is slow. Literacy is the solution to combat the huge population woes. With increased literacy, citizens get acquainted with EHR and how it works. Awareness regarding the importance of privacy in healthcare can be spread with improved literacy rates. With language also being a barrier, with increased literacy, English will be spoken by most of the population which aids the implementation of EHR. Higher literacy will drive citizens to get acquainted with the latest technology. Literacy trends in India are already showing an upward trend which further contributes to the suitability of EHR being used in the Indian healthcare system. The cloud-based system should be directly connected to the internet and updated everyone and then. A backup system is created so there is no loss of data. Multiple routes to access the data should be there so this avoids delays, interruptions, and jitters. The data should be distributed so that if there is any failure there is no total loss of data and also so that information can be accessed in pieces and a person doesn't have to wait for very long to get the information. The doctor-patient relationship can be improved if proper encryption techniques are used and data is accessed under the supervision of both the patient and doctor and decryption keys are provided after testing from both sides. Patients must have the right to control who is maintaining the data and where the data is stored. A trust should be built between the cloud service provider and the patient which ensures an agreement in which they ensure that the patient's privacy rights come first. A service level agreement (SLA) should be made between the patient and the service provider. [1] [3] [6] [11] [15]

2.	Cyberattacks	The cyber-attacks can be avoided if the records are stored separately from the base operating system and different IP addresses and network system are used so that cyber-attack is not as easy. The data should be properly protected with a strong password and no third party, for example, vulnerable antiviruses should be installed in the system. Every client should be properly verified before granting access to the information and should be immediately taken back if there is some suspicious activity from the user side.
3.	Data Sharing	A system that authorizes the administrative level and the user level is required to keep data exchange in check and under control. The administrator creates/updates/deletes the topics, authorizes the users, views data and assigns the roles to the users. At the user level, the access rights are checked and the administrator controls whether the access is granted or not and how much information is given to the user.[3]
4.	Trust in the third party	To overcome this third-party problem there has to be a neutral trusted third party that does all the encryption of the active privacy bundles and verifies the accountability of the user, stores the decryption key, provides access to the users with the data without actually getting the access to the data itself. The architecture should make privacy bundles and give the bundle to the third-party without allowing it to access the data. Therefore, the client can request access and the third-party can check its trust level without going through the personal information of the patients. This can also be done by restricting third-party access to PII. To prevent a database administrator from stealing data from the cloud which he/she oversees, the system should be designed such that the administrator can access the patient information only by patient or doctor consent. To prevent the third party from accessing PII of the patient, Advanced Encryption Standard (AES) should be used while storing data in the cloud. Multi-Authority Attribute-Based Encryption (MA – ABE) techniques for securing patient healthcare records with AES should be used. [2] [5]
5.	Infrastructure	Every client requesting data should go through a verification process. The data should be encrypted and every client should securely go through the verification process to get the decryption key so that no data should be given in wrong hands. Policies should be established that suggest which type of client can access the data and how much of the information should be shown to the client. All the data in the system should be backed up and traffic should be controlled by dividing the traffic lines, that is, by appointing multiple third parties to keep in check of these. Every client should follow specific rules to access the data for example, every client should request access first and then only further verification process will start and so on, therefore not violating the architectural policies. This makes the data secure, easily handled and under supervision. Specialists, both in the field of privacy and healthcare should be brought in and they should be involved in the decision making the process.

6.	Data Breaching	As discussed in the problems, data breaching is a major problem and the suggested solutions to this is control on the access of these records. The best method from the suggested one is the Attribute-Based Access Control (ABAC). ABAC secures the network and assigns attributes for the subject's function and authorized parties will be assigned policies with which they evaluate before granting access to any record. This allows patients to make their own policies regarding who can access these records and every client requesting for access of these records should answer a few security questions confirming their identity and accountability so that data doesn't go in wrong hands. This maintains the flexibility, accountability, security, and sustainability of the system and preserves the privacy of the patient. [10]
7.	Culture	Literacy and awareness should be spread about the need to disclose healthcare information accurately and promptly. Healthcare privacy models can only be successful when the citizens change their mindset and are willing to share their information correctly. It should be emphasized that disclosing medical data is not a weakness and shouldn't be looked down upon. Education and awareness camps should be held to inform citizens about the privacy model and the need to disclose healthcare information in a secure data environment.
8.	Prevalent Complacency	To combat slackness and laxness prevalent in India, promotion to levels of authority should be based on merit. Corruption should be eliminated and bureaucrats should be held responsible for their failures. A strict work ethic should be established and deadlines should be met. This can be done only if the mindset of bureaucrats change from doing something only for themselves to a mindset of doing something for the citizens and the country.
9.	Increased Instances of Hacking	To combat increased instances of cyberattacks on healthcare systems, a global patient identification key (GPIK) algorithm can be used. A GPIK can be used for each record using patient identifiable data. All the identifiable data, capable of identifying the individual patients is then removed from the patient record. To generate an identification key, mobile number, name, and gender of the patient can be used. Since every mobile number is unique, requires some security verification to get one and is used throughout the country it is used in forming the key. Using GPIK, even rural healthcare centers where literacy isn't high, patient's privacy and healthcare record linkage can be maintained. This solution is especially viable for developing countries like India where population density and illiteracy is high. [4]
10.	Accountability	To provide accountability in case of disclosure of private healthcare records, a specific protocol and contingency plan should be established from before to curb the data leak. Further, data and PII should be encrypted so that no sensitive information is made available even in the case of a leak. Advanced and latest encryption techniques should be implemented to preserve privacy even in the worst case of a data leak. [4]

5. CONCLUSION

Privacy in Healthcare is a desideratum to help keep patient records and identity confidential. Technological advancements in the field of healthcare are emerging at breakthrough speed. However, in most of these advancements, the security and privacy of patient data are undermined. The need for adequate security measures for patient data arises out of the fact that healthcare data is an easy target for hackers to steal identities. Also, when the patient has trust in the confidentiality of the system they tend to reveal correct information. The paper discusses the various problems which affect the successful implementation of a privacy model. The obstacles which healthcare privacy faces in India are infrastructure, complacency, cost, third party trust issues, absence of privacy policy in the constitution, etc. To rectify these issues, it requires stalwart work from the government and healthcare institutions alike. The paper weighs up on some solutions such as improvement of the literacy rate in India,

establishing accountability, making use of advanced encryption techniques, a global patient identification key, spreading awareness, etc. The future scope of the paper will be the formulation and successful implementation of a model which takes into consideration the challenges described above and finding solutions to those challenges in the most pragmatic way possible.

REFERENCES

1. Lokhande, A. R., Jamgekar, R. S., & Takalikar, R. A. Improving Privacy In Healthcare Service By Using Cloud Assisted Technologies.
2. Salih, R. M., & Lilien, L. T. (2015, March). Protecting users' privacy in healthcare cloud computing with APB-TTP. In 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (pp. 236-238). IEEE. https://doi.org/10.1109/PERCOMW.2015.7134034
3. Wadhwa, R., Mehra, A., Singh, P., & Singh, M. (2015, January). A pub/sub based architecture to support public healthcare data exchange. In 2015 7th International Conference on Communication Systems and Networks (COMSNETS) (pp. 1-6). IEEE. https://doi.org/10.1109/COMSNETS.2015.7098706
4. Khan, S. I., & Hoque, A. S. L. (2016, January). Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In 2016 International Conference on Networking Systems and Security (NSysS) (pp. 1-6). IEEE. https://doi.org/10.1109/NSysS.2016.7400708
5. Shrestha, N. M., Alsadoon, A., Prasad, P. W. C., Hourany, L., & Elchouemi, A. (2016, April). Enhanced e-health framework for security and privacy in healthcare system. In 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC) (pp. 75-79). IEEE. https://doi.org/10.1109/ICDIPC.2016.7470795
6. Deshmukh, P. (2017). Design of cloud security in the EHR for Indian healthcare services. Journal of King Saud University-Computer and Information Sciences, 29(3), 281-287. https://doi.org/10.1016/j.jksuci.2016.01.002
7. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of medical systems, 41(8), 127. https://doi.org/10.1007/s10916-017-0778-4
8. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big Data security and privacy in healthcare: a review. Procedia Computer Science, 113, 73-80. https://doi.org/10.1016/j.procs.2017.08.292
9. Md. Zahid Ibna Alam, Prof. Hiral M. Patel - Security & Privacy Issues of Big Data in IOT based Healthcare System using Cloud Computing
10. Rana, M. E., Kubbo, M., & Jayabalan, M. (2017). Privacy and Security Challenge Towards Cloud-Based Access Control. Asian. Journal of Information Technology, 16(2-5), 274-281.
11. Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. In Cybersecurity for Industry 4.0 (pp. 103-126). Springer, Cham. https://doi.org/10.1007/978-3-319-50660-9_5
12. Khan, I. U., & ur Rehman, S. (2017). A review of big data security and privacy in healthcare applications. In Big Data Management (pp. 71-89). Springer, Cham. https://doi.org/10.1007/978-3-319-45498-6_4
13. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1), 1. https://doi.org/10.1186/s40537-017-0110-7
14. Devi, R. R., & Chamundeeswari, V. V. (2018). Triple DES: Privacy Preserving in Big Data Healthcare. International Journal of Parallel Programming, 1-19.
15. Vora, J., DevMurari, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018, July). Blind signatures based secured e-healthcare system. In 2018 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE. https://doi.org/10.1109/CITS.2018.8440186
16. Kogetsu, A., Ogishima, S., & Kato, K. (2018). Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy, and Trustworthiness. Frontiers in genetics, 9. https://doi.org/10.3389/fgene.2018.00167
17. Sharma, N., & Bhatt, R. (2018). Privacy preservation in WSN for healthcare application. Procedia computer science, 132, 1243-1252. https://doi.org/10.1016/j.procs.2018.05.040

18. Sun, Z., Strang, K. D., & Pambel, F. (2018). Privacy and security in the big data paradigm. Journal of Computer Information Systems, 1-10. https://doi.org/10.1080/08874417.2017.1418631
19. Damiani, A., Masciocchi, C., Boldrini, L., Gatta, R., Dinapoli, N., Lenkowicz, J., ... & Pagliara, M. (2018). Preliminary data analysis in healthcare multicentric data mining: a privacy-preserving distributed approach. Journal of E-learning and Knowledge Society, 14(1).
20. Iyengar, A., Kundu, A., Sharma, U., & Zhang, P. (2018, July). A trusted healthcare data analytics cloud platform. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 1238-1249). IEEE. https://doi.org/10.1109/ICDCS.2018.00123
21. Vora, J., DevMurari, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018, July). Blind signatures based secured e-healthcare system. In 2018 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE. https://doi.org/10.1109/CITS.2018.8440186
22. Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management, 36(6), 1161-1173. https://doi.org/10.1016/j.ijinfomgt.2016.07.006
23. Senthilkumar, S. A., Rai, B. K., Meshram, A. A., Gunasekaran, A., & Chandrakumarmangalam, S. (2018). Big data in healthcare management: a review of literature. Am. J. Theor. Appl. Bus, 4, 57-69. https://doi.org/10.11648/j.ajtab.20180402.14
24. Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for iot and cloud-based healthcare systems. IEEE Internet Computing, 22(2), 42-51 https://doi.org/10.1109/MIC.2018.112102519
25. Narayan, S., Gagné, M., & Safavi-Naini, R. (2010, October). Privacy preserving EHR system using attribute-based infrastructure. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (pp. 47-52). ACM. https://doi.org/10.1145/1866835.1866845
26. Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. Healthcare informatics research, 22(3), 156-163. https://doi.org/10.4258/hir.2016.22.3.156
27. Ould-Yahia, Y., Bouzefrane, S., & Boucheneb, H. (2018, April). Towards privacy and ownership preserving of outsourced health data in IoT-cloud context. In 2018 International Symposium on Programming and Systems (ISPS) (pp. 1-6). IEEE. https://doi.org/10.1109/ISPS.2018.8379018
28. framework for RFID based healthcare systems. Future generation computer systems, 72, 339-352.
29. Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Information Sciences, 479, 567-592. https://doi.org/10.1016/j.ins.2018.02.005
30. Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2019). Secured data collection with hardware-based ciphers for iot-based healthcare. IEEE Internet of Things Journal, 6(1), 410-420. https://doi.org/10.1109/JIOT.2018.2854714
31. L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, vol. 10, no. 5, pp. 557–570, 2002 https://doi.org/10.1142/S0218488502001648
32. Sweeney, "Uniqueness of simple demographics in the U.S. population," 2000.
33. Xu, L., Jiang, C., Chen, Y., Ren, Y., & Liu, K. R. (2015). Privacy or utility in data collection? A contract theoretic approach. IEEE Journal of Selected Topics in Signal Processing, 9(7), 1256-1269. https://doi.org/10.1109/JSTSP.2015.2425798
34. Website: https://www.ihs.gov/ndw/ last accessed: 13th July 2019.