A Review on Privacy Preservation Techniques in Surveillance and Health Care Data Publication

Pavan Kumar Vadrevu[1], Sri Krishna Adusumalli[2], Vamsi Krishna Mangalapalli[3]
Sangram Keshari Swain[4]
1Assistant Professor, Department of Information Technology, Shri Vishnu Engineering College for Women, Bhimavaram, Andhrapradesh
2Associate Professor& HOD, Department of AI&DS, Shri Vishnu Engineering College for Women, Bhimavaram, Andhrapradesh
3Professor, Department of CSE, Chaitanya Institute of Science and Technology, Kakinada. Andhrapradesh
4 Associate Professor, Centurion University of Technology and Management, Bhubaneswar Campus, Orissa

Abstract: ***This manuscript focuses on the state-of-art related to privacy preserving data publication. Usually, data is classified into Relational data, Transactional data, Set-value data, Trajectory data and Social Network data etc. In this script video surveillance data and healthcare data is considered. This manuscript is divided into two parts. First, different privacy preserving anonymization operations on video surveillance data is discussed. Second, the existing personal privacy preserving methods of healthcare data publication are given. Finally, the pros and cons of existing privacy preserving models in surveillance and continuous medical data publication are discussed.***

Keywords:surveillance data, health care data, privacy preservation.

PrivacyPreservation in Video Surveillance Data

Now a days the video surveillance system is a serious tool for various responsibilities like personal safety, securing the assets, resource monitoring & planning, traffic control, law enforcement etc., However, the increasing use of cameras in surveillance task has presented serious privacy concerns. Every person and activity are continuously being monitored in the offices, parking lots, roads, supermarkets, other commercial environments, etc., This increase monitoring like observing your private moments, identifying the people with others at a specific time or place, eavesdropping on every day activities etc. The video surveillance with
privacy-preserving will handles these requirements of utility and confidentiality.

Presenting security and privacy in visual data processing was endeavored with reasonable
success in various domains. The smart cameras implement surveillance itself or cover the sensitive
or confidential information in videos. The smart cameras need cost efficient programmable and are restricted to individual camera algorithms. The homogenous owner's leads privacy issues and vulnerabilities while analyzing multiple flows from different cameras deployed in the city.
The camera settings, video frames and time stamps are possibly tampered by the malicious users digitally.

These manipulations lead to violating the privacy of the neighbors. The law enforcement agencies strongly depend on the video surveillance system as the one of the evidences on a considerable scale.The researches define various privacy-preserving protocols to address the several privacy concerns of video surveillance against live feed of malicious database. The latest video surveillance systems offer techniques to contest security threats and the privacy of the individual persons under surveillance are greatly affected by the advanced features of these surveillance systems. The cryptographic mechanisms are adopted to protect the privacy from the external attackers to secure the video streams and also it is important to protect the data from the internal persons. Allowing applications for full accessing of video data discloses wide range of information than it originally required to implement their functionalities and it prone to a privacy risks to the individuals.

The IoT is getting more dominating when amount of internet connected devices are increased and volume of data received by the IoT sensors also very high and required efficient data processing and analytical method to validate the privacy of the data collected. Video surveillance requires the cloud for storage, accessibility and processing power from various ends of the world to any devices. For such systems, the cameras just collect the video data, stream to the cloud and it stores the data, implements motion detection, analyses the video data and sends the alerts to the users. The cloud based base service providers like cloud-based surveillance system receives the data in raw format from the users. Where the surveillance system continuously records the people daily life and it creates the doubt on the user privacy.

The extensive use of biometric systems increased the privacy concerns, specifically while implementing the Privacy-Enhancing Technologies at untrusted servers or central systems to perform biometric matching. The challenge of presenting security and privacy in surveillance systems in government or private organizations has major threat to the visitors and employee's personal privacy. Majority of the solutions suffered with high computational and communicational overhead.

State of the art Methods

In this [1] article, authors proposed a methodology for H.264/AVC bit streams, which implements a motion detection and tracking in encrypted format. The advantage of the proposed solution is firstly, the algorithm for motion detection is applied on compressed encrypted domain and it does not require the decryption or decoding of bit stream which is suitable for real time video application. Secondly, motion region is obtained by using skillful estimation and physical priors of the object and got 0.90 F1-score for detection, which provides high speed detection on motions.

The experimentation proved that detection rate exceeded more than 100 frames/sec. Finally, without effecting the detection accuracy and detection speed the proposed method can be applied to the conventional encrypted video and videos encrypted with other formats of bits teams to preserve the personal information of the users. The proposed method is well suitable for cloud home care, forensics and cloud video segments. In the cloud applications the privacy is maintained by encrypting the information and that do not require to download and decryption of the same for verification. The balance between privacy and convenience is achieved easily, because the cloud does not required decryption for information in motion detection.

The proposed method failed to maintain the consistency in detection speed and accuracy, because the performance of the approach is depending on the type of cryptographic algorithm used, number of keys, number of rounds and size of the key. And also, storage requirements for this approach are very high to accommodate the sensitive or motion data. It requires additional efforts to improving motion detection to preserve the confidentiality for crowded scenes and for scenes of sensible movements with camera. In motion video anomaly detection plays a vital role in preserving the privacy, this is not addressed by the proposed method.

The cloud based base service providers like cloud-based surveillance system receives the data in raw format from the users. Where the surveillance system continuously records the people daily life and it creates the doubt on the user privacy. Therefore, need of intelligent analytics for privacy-preserving the user information is essential. In [2] the authors proposed homomorphic encryption approach to study the moving object detection in cloud-based video surveillance system with encryption for privacy preserving. This homomorphic encryption approach validates the operations on between encrypted and unencrypted data. The advantage of the proposed approach is more secure and efficient with real time analytics of encrypted video streams in motion detection or moving object detection. The drawback of the proposed method is it is not practical and requires high storage due to terrible computations. The proposed method uses Paillier cryptosystem which slowdowns the performance and consumes more time for processing, because it needs 1024 bits to represent each pixel rather than 8 bits in traditional approaches.

In [3] the authors proposed a method for video surveillance scenario known as privacy-preserving watch list screening system. It was designed to differentiate interested group of identities without authorizing specific identity preciously by ensuring anonymity in people. The proposed method uses the homomorphic cryptography during the screening process to prevent the exposure of private information such as images of faces. A simplified approach is adopted to evaluate the threshold comparison and the complexity of the proposed system is reduced with systematic solutions. The experimentation reveals that the proposed method is feasible for piracy preserving in video surveillance with facial images and acquire reasonable accuracy and low complexities. The advantage of the proposed method is it improving the privacy in video surveillance system. The main goal of these is to maintain the individual privacy with identifying the people and personal information of them with facial recognition. The drawback of this proposed method is it considers only the facial image of the people in video surveillance and optimization of the homomorphic cryptosystem is required to improve the performance and accuracy.

The extensive use of biometric systems increased the privacy concerns, specifically while implementing the Privacy-Enhancing Technologies at untrusted servers or central systems to perform biometric matching. In [4] the authors proposed a privacy-enhanced face recognition system that hides the server results and biometrics efficiently and implements the matching operation with secure multiparty computation technique. They introduced a protocol which match the encrypted facial image over the database of facial templates and the detection result and biometric itself where hidden from the server while implementing the matching process. The approach is twofold where one party collects and supplies facial images and other part gain the access to a facial template database. The proposed approach uses Eigenfaces recognition algorithm in which the first party does not know additional information at the time of protocol execution from the database and other party cannot know the result of the processing system and input images. The advantage of the proposed method is it is well suitable for executing in conventional hardware. With extensive experimentation it is evident that privacy-preserving algorithm proposed is reliable and that the execution is also feasible on present hardware platforms. The detection rate achieved with this method is more than 96% for facials recognition. A drawback of the proposed system is it is very difficult to run on encrypted images and very complex scenario to adopt.

In [5] the authors introduced a high-speed method to video surveillance for H.264/AVC compressed video to detect moving objects accurately. Unlike the traditional approaches the proposed approach does not rely on the compressed bit streams. The background model is constructed effectively in training phase is proportional on the number of bits used by the MBs. The images are filtered specially and temporally with the regions of interest are defined with the MB sizes of the new images. The detection result is refined with 4X4 transformation coefficients of the MB images. The advantage of this approach is to maintain good precision and recall values compared to other MV values. The drawbacks of the proposed method are it is restricted to system level and high execution time is exhibited but failed to maintain for other requirements.

Allowing applications for full accessing of video data discloses wide range of information than it originally required to implement their functionalities and it prone to a privacy risks to the individuals. In [6] the authors focused on visual recognizer applications and offered privilege-separation architecture that encourages the recognizer logic least privilege separating technique and modularization. The network access and file system is restricted with sand boxing from extracting the raw video data. The proposed approach uses a protocol which splits the application modules and recognizer and evaluated the proposed architecture with 17

computer-vision applications. The experiments reveal that the proposed method has low overhead and minimizes a limited privacy risk. And, with the increase in parallelism and concurrency the performance of the proposed method is increased. The drawback of this approach is, it is very difficult to implement, but it offers major privacy and security benefits.

The challenge of presenting security and privacy in surveillance systems in government or private organizations has major threat to the visitors and employee's personal privacy. Majority of the solutions suffered with high computational and communicational overhead. In [7] the authors proposed a framework to provide privacy to the surveillance system efficiently. The frame is divided into group of images and each image does not contain useful information, but this group of images holds meaningful information. The proposed approach is derived from the Chinese Remainder Theorem applied to the images and derived the solution. The proposed method uses distributed storage and processing securely and contains the ability to reconfigure the data to satisfy legal requirements. The advantage is it can effectively track and detect people and various survival tasks. The approach is practical and more efficient compared to secure multiparty computation. It is not addressed change detection, optical flow and face detection of persons in surveillance while providing the privacy. It depends more on the distributed systems and the privacy and security of these distributed systems are not guarantee in the surveillance process.

The raise in the privacy risk is addressed the authors [8] in context-aware or perceptual applications which monitors or tracks the user activities and environment with cameras and other alternative sensors. The authors design a practically feasible privacy protection mechanism referred as DARKLY for an untrusted perceptual application executing on a trusted device by the third party. The proposed DARKLY is attached with the OpenCV library used to access visual inputs with the applications. The algorithm privacy transformation, access control and user audit were included as a multiple privacy protection mechanism in DARKLY. It implements diversified tasks such as object tracking, image recognition, and face recognition and security surveillance. The advantage of the proposed method is it implements all these tasks with minimal overhead compared to OpenCV. In all these cases the application accuracy and functionality are not decreased. Drawback of this is in some scenarios the privacy and utility should be automatically acceptable by considering the strong privacy protection. Supervised machine learning approaches are used to build filters and constructors for delicate and privacy-sensitive scenes which include gestures, movement patterns, physical proximity and text strings. It is failed to handle various types of audio data.

To enable various security measures, the CCTV with intelligent security environment is required to improve the performance of video surveillance system. This leads to the privacy protection problem for surveillance system. The authors [9] addressed the leakage of personal information from the surveillance video which causes the violation in privacy to the severe social issues. This intelligent surveillance mechanism exhibits adverse results like exposure of privacy, data manipulation, etc. The authors proposed block-chain based data processing approach for videos and synchronize huge data securely and in the delivery process the data is stored. The advantage of this approach is, it does not expose the privacy in the synchronized operation, because it protects from the forgery or falsification attacks efficiently.

The authors also proposed SM-Tree approach, because the existing methods does not protect from the message interception, whereas in SM-Tree the message are encrypted and these are protected. The proposed method minimizes the bandwidth essential for transmission and also offers minimum cost for reduplication storage. The privacy of the object is garneted, because the decryption is adopted at the masking side and the encryption is used at the synchronization process. The drawback of the proposed approach is, less efficient for high quality images or video. This a privacy violation in the surveillance process of CCTV and required secure counter measure. Further refinement is needed in privacy masking and algorithm of reduplication.

The homogenous owner's leads privacy issues and vulnerabilities while analyzing multiple flows from different cameras deployed in the city. The camera settings, video frames and time stamps are possibly tampered by the malicious users digitally. These manipulations lead to violating the privacy of the neighbors. The authors addressed [10] these problem and proposed block chain base solution called as BlockSee, which promises the integrity of the surveillance videos and their configuration and provide availability of the data to the officials without uncontrolled discovery. The privacy is impacted greatly with tampering of camera settings and allows the people to identify the probable violations of their privacy life. The advantage of these Block See is, it joins computer vision and block chain technology to focus on the transactions including the exchanging of video segments. The drawback of this approach is it failed to identify the obfuscated version of the scene or video and it requires exclusive computer vision techniques. Implementations of BlockSee require storing of data in metadata format as multichain streams and considering the same for exchanging the information.

The IoT is getting more dominating when amount of internet connected devices are increased and volume of data received by the IoT sensors also very high and required efficient data processing and analytical method to validate the privacy of the data collected. The authors [11] addressed the same and proposed edge computing-based approaches to process the data closer to the sources to protect the privacy. But practically and economically it is not possible to fix a dedicated resource to the infrastructure every time. The authors proposed decentralized IoT edge processing system and it solved the problem of edge processing for privacy preserving. Advantages of this method are it addresses the scaling needs of the system to maintain privacy. Drawback of these is it is practically very difficult to implement and also cost effective.

The authors [12] proposed block chain-based video surveillance system with the assumption of internal managers with blockchain network. The IP cameras are used to record the videos and these encrypted recorded videos are stored in IPFS using blockchain network with trusted administrators.

The decryption key is stored in the database of the specific node and implements authentication, where the internal manager does not use the decryption key. The approval is required from the block chain network or manager, whenever any person needs to view the video and the manager runs the chain code for exporting the video. The decryption key is used to generate the license in chain code API based on the browsing time and reading period. The advantage of the proposed system is it can easily manage videos from internal administrators and external persons. The drawback of this system is, there is a possibility to leak the data or keys by the internal managers when they are compromised.

Video surveillance requires the cloud for storage, accessibility and processing power from various ends of the world to any devices. For such systems, the cameras just collect the video data, stream to the cloud and it stores the data, implements motion detection, analyses the video data and sends the alerts to the users. The authors [13] addressed cloud video surveillance with privacy-preserving motion detection technique. The motion trajectories and the shapes of the moving objects are identified from encrypted video and the bit rate of the original compressed video with HEVC is same as the encrypted video with good compression efficiency. The design combination of encryption and detection stabilizes leakage in privacy and utilization of data for privacy-preserving without considering the homomorphic encryption. The limitation of the proposed approach is it allows only one cloud to store the video data and authorization is required every time to access the cloud. The advantage is the computational complexity is very low compared to traditional approaches.

Video surveillance, IP camera and CCTV become crucial for much government, private organizations or businesses and individual users to track the privacy of the individuals. Privacy preserving in these systems become a complex and challenging task. Nevertheless, researchers focus on the privacy aspects of such systems. The authors [14] used publicly available data to review the existing threats in various surveillance systems. The insights find in this study helped to develop the system to tackle the privacy risks. Finally, the authors listed the collections of recommendations which are helpful to improve the privacy and security in hardware, network communications and video surveillance operations.

The video surveillance system attempts to protect privacy information of the users without disturbing the regular surveillance tasks and maintains the reasonable accuracy and efficiency. The authors [15] addressed the regions of privacy and proposed a system a novel notion-graph to protect the privacy regions of user protection privacy in cloud video surveillance. The proposed novel notion and concept graph defines user privacy requirements and further these can be applied to design event distiller model along with privacy interface model to determine privacy policies. The proposed privacy regions are mapped with conditional random fields of video frames and resultant findings. The Patronus was evaluated with real world privacy settings and defined the efficiency of privacy protection without minimizing the systems surveillance functionality.

The authors proposed [16] an adaptive approach in which the data transformation cleverly hides sensitive information in the video with consistent video quality and maintain strong privacy. The authors discovered adaptive transformation scheme in CCTVs to exploit the global transformation benefits, whenever it is used with the output of unreliable third-party detectors. In proposed approach the pixelization is better than blurring and converting static evidence regions with 8% less falsehood than blurring and 55% less falsehood than quantization. Compared to selective complication methods the proposed method is more reliable and compared to global conversion poses it holds 38% less visual distortion. Blurring holds 11% less falsehood than pixelization, when it performs foreground transformations with operations related space variant. The drawback of the proposed method is, this is not tested and adopted for the real time environment for validating the privacy and distortion. And, it is very difficult to know the amount of distortion accepted by the surveillance system and mechanisms are required to handle dynamic background and foreground.

The law enforcement agencies strongly depend on the video surveillance system as the one of the evidences on a considerable scale. The researches define various privacy-preserving protocols to address the several privacy concerns of video surveillance against live feed of malicious database. But the authors [17] proposed a system that made easy of getting information when a face image is matched with the law enforcement's database by considering the privacy requirements. The proposed approach exposes a random variation of obfuscated scores and these obfuscated score exposes least information about the original score. The advantage of the proposed method is it protects the privacy of the facial data, in spite of compromised security descriptions. However, the proposed protocol establishes a single line of communication between server and the camera and it exhibits the online computation time for a database 100 suspects at server and camera as 34ms and 155ms.And the communication cost for online transaction is recorded as 12KB. Finally, the proposed method offers strict privacy assurances and, as a result, they are well scalable for ubiquitous deployment.

The wide-spread usage of video surveillance systems disturbing the personal aspect of individual citizens and affecting their personal privacy. To address these issues the authors [18] proposed personal image and video protection mechanism tools. The effectiveness of these tools on the surveillance tasks is greatly impacted. The individual user evaluation is done with crowdsourcing to explore the balance between the privacy preservation accessible with tools and the perspicuity of events in video surveillance. The proposed method is outperformed compare to that of existing traditional approaches such as pixelization, masking and blurring adapted to video surveillance. The proposed idea is evaluated using Facebook crowdsourcing application and particularly designed to evaluate the subjective data. The privacy protection and intelligibility are well balanced and proved the same with experiments conducted on one hundred participants. The results of the crowdsourcing application are correlated with traditional convolutional tests and proved that these are efficient.

The authors [19] proposed a well-organized framework for Internet of Multimedia Things (IoMT) as applications privacy-preserving-based data collection and analysis (P2DCA). In IoMT the multimedia video surveillance systems are suitable to define both multimedia and non-multimedia data. The captured data is sent to Base Station (BS) of cloud server and possibility of disturbing this is very high to distrust the privacy. Several privacy issues were exposed such as exposing the identities and MSNs location information and need for privacy-preserving in MSNs are very high in mobile data collections. This framework divides the multimedia sensor network as multiple clusters and each cluster is responsible for a cluster head. The privacy of the member MSNs is handled by the heads with the help of coordinate aggression and location data. The cumulated multimedia data is evaluated with cloud server through counter-propagation ANI and segmentation is used to extract the useful information. The experimentation reveals that the proposed method is more efficient than traditional privacy-preserving schemes and practical to extract the data from MSNs.

The growing of video surveillance system in civilized areas forced to attain the privacy preserving of personal information. The authors [20] formulated a training framework to extract the anonymization transform for captured videos, so that it is explicitly optimized anonymized videos between the associated privacy budgets and performance of target utility task. The task driven contexts are used to define privacy budget which consistently designated to individual model performance and privacy must be withstand beside every malicious model that tries to theft various information. The authors proposed two novel optimization techniques such as restarting and ensemble to achieve tougher global privacy protection against various attacker models. Widespread experimentations have been conceded and analyzed. The authors assumed that the multiple single task datasets for experimentation of original investigative for cross-dataset training and evaluation.

The mass-surveillance system prone to privacy breaches due to the exploits of vulnerabilities by opponents and exploitation of cameras. This leads the need of privacy preserving of data in surveillance systems. The authors [21] proposed lightweight dynamic chaotic image enciphering (DyCIE) based privacy preserving algorithm for selective video surveillance approach called as PriSev. The PriSev is combined with object scanner, very agent-based key and DNN based frame classification models. The DyCIE technique offers an end to end enciphering of video frames that holds objects to block privacy gaps identified with interceptions. The DNN based model categorizes frames into aggressive and innocuous for designing positive conditions to filter criminal or aggressive or no criminal patterns that protects from the privacy holes caused with leakage of the authorized people in the surveillance system. The advantage of the proposed system is it exhibits good accuracy and efficiency. Particularly the DyCIE method is very faster than existing traditional approaches.

The authors [22] defined that the best privacy protection and low privacy insensitivity cannot be attained with minimization of data. Collecting additional information is essential for data anonymization in some tracking scenarios. They are concluded that additional data is utilized only for protecting privacy and not possible to access and use in another context. Hence, these additional data improve the privacy level and improved the selective surveillance. The new intelligent based video surveillance system has been developed in collaboration with engineer and lawyers.

The authors proposed [23] person detection with operational verification for privacy-preserving in video surveillance system. The sensor in the proposed approach identifies the person face and position as a one-dimensional brightness without using two-dimensional image data. The brightness distribution information is enough to distinguish the position of the person and it does not hold the complete information about an individual person. It leads to the detection of the person position accurately without knowing the complete information of the person or even the facial image information's. In the proposed work, the detection sensor was placed horizontally to detect the position of the person and detects the position as the person is fallen or standing. However, if multiple sensors are fixed on the ceiling as orthogonal position and it can detect the positions of multiple persons.

The latest video surveillance systems offer techniques to contest security threats and the privacy of the individual persons under surveillance are greatly affected by the advanced features of these surveillance systems. The cryptographic mechanisms are adopted to protect the privacy from the external attackers to secure the video streams and also it is important to protect the data from the internal persons. To accomplish these requirements the authors proposed [24] secure video surveillance system. The existing video surveillance system for security and authentication in multimedia systems are not fulfilled these requirements to maintain the personal privacy.

Pros and Cons of privacy-preservation in video surveillance data

In this section, the analysis is done for security and privacy challenges in protecting personal information in video surveillance data from the discussion of various existing methods and techniques for various organizations are highly beneficial in attaining privacy and security. This section presents various approaches and methodologies from different papers with the emphasis on their advantage and limitations. The limitations of various methods are consolidated as below:

- Many approaches used the encryption mechanism to provide security, but for protection of large-scale video data from multiple sources is require innovative efficient real-time encryption algorithms.
- Duration-specific key management techniques should be adapted to maintain privacy and security with encryption techniques for the data captured by numerous cameras.
- Need of Secure storage of video data and the related metadata is required, whenever facilitating effective retrieval of the stored data.

- Mechanisms are required to protect the data from Integrity attacks and these solutions should have robustness against gentle modifications.
- To handle large-scale video surveillance data effectively, Scalable and efficient authenticity mechanisms are required.
- Using the existing privacy enhancing techniques to implement multiple privacy levels in the video surveillance data where every level is accessible to various access privileges.
- Privacy-preserving of user's information requires dynamic access control to protect from exposing of maximum information to the operators when required.
- Innovative access control mechanisms are needed to exploit the indexing structure of video data to extract the metadata.
- Combined identity and access management techniques are required to access the authorization of video surveillance data.

Privacy-preservation in Healthcare data

The rapid development of the electronica health record system increases the necessity of collecting the health data at an unpredictable rate. The sharing of these collected health data among various parties and applications become essential such as policy development, data mining and decision support systems. However, the major challenge is sharing of these health data is protecting individual privacy and the present scenarios depends on the guidelines and polices defined for sharing of the personal health data. For example, the Health Insurance Portability and Accountability Act (HIPAA) of USA describe two methodologies to attain de-identification. Firstly, the expert fortitude that involves an expert to confirm the de-identification threat essential in the data is necessarily low. Second is Safe Harbor that needs conquest and deletion of attributes and it delete particular information to de-identify the records with the support of data disclosures checklist. Though, there are several arguments and privacy debate on HIPAA privacy rules both sides. Many people stated that the de-identification data is insufficient to provide the protection and others vie that these privacy protections hinders biomedical research.

Several scenarios where evolved to protect the privacy-preserving of personal healthcare data and some of the areas and domains along with the suggested solutions from the literature are explained in this section. Web-based Media Health Networks give a promising worldview to attract patients to share and impart their personal health status with other online patients and consult medical care administrations from online custodian with social networks. However, how to create the trust among patients and custodian raises a difficult issue because of the transparency of the interpersonal organizations, in the interim the personal privacy might be unveiled when offering personal health data to different patients and custodian.

Similarly, in IoT-based medical services, clinical devices are more vulnerable against various security threats and attacks than other network devices. To some extent, Current solutions are able to provide protection to patients' information during information transmission somewhat, but unable to prevent some of the sophisticated attacks and threats such as collusion attacks and data leakage.

The electronic medical care (e- health) framework has been advanced into a patient-situated assistance with more modest and smarter wireless devices. As these smart devices have restricted computational capacity and memory size, it is harder to secure the client's enormous private information in the e-health framework. Albeit a few works have established a secure session key between the client and the medical server, the security shortcomings actually exist in preserving the anonymity with low energy utilization. In addition, the abuse of biometric data in the key agreement process may prompt privacy disclosure, which is unsalvageable.

Conveniently, Medical services through tele-care medication data frameworks (TMIS) can assist patients with acquiring their desired telemedicine services. However, data security and privacy protection are significant issues and crucial challenges in medical services data frameworks, where just approved patients and doctors can utilize telecare medication facilities and access clinical records electronically. Consequently, secure authentication scheme is urgently needed to accomplish the objectives of data confidentiality, entity authentication and privacy protection.

State of the art methods

The major challenge for health care domain is providing privacy for the health care data and maintaining confidentiality to the personal information. The mining community does not given importance to these until the community has designed several privacy-preserving transformations in the data mining. But not all these tools and techniques are applicable to process data and the authors [25] analyzed the privacy of personal information and requirements for processing health care data and explored the appropriate privacy-preserving method to anonymize the sensitive data. The authors validated these methods with several process mining results on the health care data logs in the public environment. The experimentation reveals that the performance of these anonymization methods varied with respect to the algorithms and health data used. The authors proposed framework for privacy-preserving of healthcare data by using meta data and validation of healthcare process. The advantage of the proposed approach is they are using framework with traditional privacy preserving techniques to protect the personal healthcare data and validated with the meta-data. The performance of the proposed method of privacy-preserving is high and very efficient. The drawback of the method is not suitable for the real time traffic and cannot identify or address the privacy requirements of process model.

Process mining has been effectively applied in the medical domain and assisted with revealing different experiences for improving medical care processes. While advantages of process mining are generally recognized, numerous individuals legitimately have worries concerns about irresponsible utilization of individual information. Medical care data frameworks contain exceptionally sensitive data and medical services guidelines often require protection

of privacy of such information. The need to comply with strict privacy necessities may bring about a diminished information utility for analysis. Despite the fact that, recently, data privacy issues didn't get a lot of consideration in the process mining community, many privacy-preserving data transformation strategies have been proposed in the data mining community. Numerous similarities between data mining and process mining exist; however, there are key contrasts that make privacy-preserving data mining methods unsatisfactory to anonymous process data. In this [26], we examine data privacy and utility necessities for medical services measure information and evaluate the reasonableness of privacy-preserving data transformation techniques to anonymize medical care data. We additionally propose a structure for privacy-preserving process mining that can uphold medical care process mining analyses.

Web-based Media Health Networks give a promising worldview to attract patients to share and impart their personal health status with other online patients and consult medical care administrations from online custodian with social networks. However, how to create the trust among patients and custodian raises a difficult issue because of the transparency of the interpersonal organizations, in the interim the personal privacy might be unveiled when offering personal health data to different patients and custodian. In this [27], we have proposed a customized and believed medical care administration technique to deal with empower trusted and privacy preserving medical services administrations in web-based media networks. The proposed approach can improve the trustiness among patients and custodian through genuine appraisals towards custodian. Collaborative filtering model is applied into the proposed method to deal in finding caregivers through contrasting the health symptoms with different patients. Moreover, we build up a Sybil attack detection technique to prevent patients' fake evaluations and audits. Extensive performance assessment results dependent on real data sets show that the proposed approach can precisely match the patients and proper caretakers, as well as effectively resist detection of Sybil attacks in adequate time consumption. In future the work can be further extended to improve the efficiency of the detecting Sybil attacks. Performance assessment shows that this methodology can accomplish prominent performance improvement; regarding finding personalized parental caretakers and resistance to Sybil attacks.

Healthcare information is frequently maintained by various organizations. However, sometimes detailed analyses require these datasets to be incorporated without disregarding patient or business privacy. Multiparty Private Set Intersection (MPSI), which is a significant privacy-preserving protocol, processes an intersection of different private datasets. This methodology guarantees that only designated parties can distinguish the convergence. The proposed [28] a practical MPSI in which a portion of the calculations are outsourced to a third-party. As none of the data of Si, |Si| ($\forall i \in [1, n]$) is revealed to the third-party, this function can be securely outsourced. This methodology satisfies the following requirements: any limitations on the sets are disposed of, implying that the set size of every player can be deftly picked; and the computational weight on every player is autonomous of the number of players. Significantly, this methodology can be applied to the efficient integration of clinical and related information maintained by various associations without disregarding any protection limitations. We affirmed that the computational complexity is independent of the number of organizations from which information are being coordinated. This MPSI depends on the use of outsourcing provider, who has no information on the data inputs or outputs. This diminishes the computational complexity. The performance of the proposed MPSI is assessed by executing a model on a virtual private network to empower parallel computation in multiple threads. This protocol affirmed to be more effective than existing methodologies.

In IoT-based medical services, clinical devices are more vulnerable against various security threats and attacks than other network devices. To some extent, Current solutions are able to provide protection to patients' information during information transmission somewhat, but unable to prevent some of the sophisticated attacks and threats such as collusion attacks and data leakage. In this [29], an investigation is carried out on privacy protected data collection and access in IoT-based medical applications and proposed a new framework called Privacy Protector to safeguard the privacy of patients' personal information. At that point we have introduced a secret sharing approach named SW-SSS so as to optimize the secret share size and to support exact-share repairs while as yet maintaining the benefits of the previous approach. The approach devises the patients' information and stores it in a several cloud servers. If one or two data servers are compromised, the patients' personal information privacy is as yet ensured. For medical care suppliers, we present a patient access control approach, where several cloud servers team up to offer patients' information to medical care suppliers, yet don't uncover the content of the information. The performance analysis shows that the Privacy Protector framework is secured against different attacks and threats.

In Internet of Things (IoT), there are incredible security concerns with patient health monitoring sensors. By recent sophisticated security and privacy attacks, the concerns are also become conscious including data breaching, data integrity, and data collusion. During the patients' health monitoring data communication, Conventional solutions often offers security. In this [30], based on the investigated challenges in safe information collection procedure for IoT based healthcare applications and frameworks, a new scheme named Secure Data is proposed with the aim to handle security concerns like the above mentioned. The proposed scheme provides data security and preserves the privacy of the patients' personal information. KATAN secret cipher algorithm is implemented and optimized it on the FPGA hardware platform for secure communication. Secret cipher sharing and share repairing is applied for ensuring the privacy of the KATAN cipher. When to apply against attacks, Secure Data performance analysis shows, this scheme is efficient in terms of frequency, energy cost and computational cost. In future, the proposed scheme can be implemented with different metrics and analyze the algorithm under different threats and attacks when applied to specific applications.

With the progressions in electronic medical equipment, e-medical services framework becomes a promising paradigm to consistently monitor health conditions and analyze phenomena remotely. However, it additionally creates a huge volume of health information and poses many security challenges, like privacy leak age and access control security. Moreover, several clinical devices/sensors have low battery power. In this [31], lightweight privacy preserving fog-assisted information sharing scheme (PFHD) for large health information is proposed to provide fine-grained access for information proprietors. Initially, proprietor's shared information is categorized into profile and health information and encodes them with various encryption algorithms. Second, the health information is re-encoded with a new access policy by the fog server. Security conversations show that PFHD can accomplish fine-grained information sharing with privacy preservation. Performance assessment shows that PFHD can be applied into resource-limited e-medical care framework with efficient encryption trouble burden in terms of storage and computation cost. As a future work, an outsourcing decryption scheme can be developed to reduce the cost for decryption.

As medical organizations become more associated and digitized (e.g., digitization of patient records, medicine or prescription requesting, correspondence among specialist doctors and patients), guaranteeing the security of Internet-enabled devices and the framework without trading off performance and ease of use also become increasingly challenging. Software-defined networking (SDN) permits the decoupling of network control from the data plane, yet SDN based solutions are not commonly intended to moderate against insider threats/attacks. In this paper, the authors reviewed stakeholders from 12 medical organizations in Hong Kong, Singapore and China to get in-depth comprehension of the framework design requirements in medical networks. Inspired by our discoveries, the authors [32] focused on proposing a trust-based Bayesian approach for identifying the insider attacks in healthcare SDNs environments. in collaboration with two of the 12 healthcare organizations, Discoveries from our assessments in both simulated and real-world environments showed that the adequacy and adaptability of our methodology in detecting malicious devices under different conditions. As a Future work of the above proposed approach, further investigation could be towards the improvement detection sensitivity and validating the performance of the approach in an even larger environment.

Over a decade, the electronic medical care (e-health) framework has been advanced into a patient-situated assistance with more modest and smarter wireless devices. As these smart devices have restricted computational capacity and memory size, it is harder to secure the client's enormous private information in the e-health framework. Albeit a few works have established a secure session key between the client and the medical server, the security shortcomings actually exist in preserving the anonymity with low energy utilization. In addition, the abuse of biometric data in the key agreement process may prompt privacy disclosure, which is unsalvageable. In this [33], a three-phase dynamic authentication key agreement scheme mechanism for e-health frameworks is proposed to ensure the client's privacy. Two-factor schemes introduce weaknesses in performing biometric authentication at the server. To give intractability and with the goal that the client anonymity can be fully preserved, the conventional identity-password table is supplanted by a dynamic verification table. Moreover, our mechanism adopts lightweight hash and bio-hash operations, which decreases the computational expenses and correspondence costs in comparison with other techniques in the literature. We likewise demonstrate the proposed mechanism to be semantic secure under the Real-or-Random Model. Hence, the proposed mechanism can satisfy the energy utilization needs and security needs of e-health frameworks effectively.

Conveniently, Medical services through tele-care medication data frameworks (TMIS) can assist patients with acquiring their desired telemedicine services. However, data security and privacy protection are significant issues and crucial challenges in medical services data frameworks, where just approved patients and doctors can utilize tele-care medication facilities and access clinical records electronically. Consequently, secure authentication scheme is urgently needed to accomplish the objectives of data confidentiality, entity authentication and privacy protection. This paper [34] examines a novel biometric verification scheme for tele-care medication information systems (TMIS). We consider patient's secrecy and secure clinical information transmission in biometric authentication scheme to oppose several attacks. In addition, to construct an enhanced scheme hash function, fuzzy extractor, nonce, and authenticated Diffie-Hellman key agreement are employed as the primitives. It safeguards clients' privacy and accomplishes forward secrecy of session key. Besides, the analysis shows that the new scheme improves the data security and patient privacy. Finally, the tradeoff among security and effectiveness answers on the actual prerequisites for patient demands and framework policies in viable application.

The authors [35] proposed Personal Health Information (PHI) based on the patient-centric approach to share and access the personal information referred as SPS. The SPS is designed for cloud and it is more secure and efficient than the traditional mechanisms. The SPS uses patient’s pseudo identification and digital signature in attribute-based cryptography to provide the privacy and security to PHI. The additional responsibilities of the health service providers are reduced by storing the PHI data in cloud and reduced the maintenance cost with this storage to electronic Health care systems. The SPS assigns different attributes based on the roles and relationship with the patient to access requester of PHI, because it adopts the attribute-based encryption method for processing the data. The SPS adopts multi party proxy re-encryption protocol for providing the authenticated access to PHI with normal computation cost. The processes are efficient because of usage of Light weight partial and block PHI and it provides integrity and availability services. The experimental result shows that SPS meet the desired security requirements and poses high efficiency and more secure with low storage cost. The advantage of proposed scheme is highly efficient to counterattack several probable attacks and malicious behaviors.

The remote monitoring of the patients is now a day is possible with advances in sensor networks which reduce cost and patients experience the high-quality health care services. The alerts are generated when the heartbeat or pressure exceeds or lowers the defined threshold value. But transmitting these values from the patient to the sensor prone to security violation and vulnerable to privacy threats which should be consider seriously. The traditional solution to counter this problem is cryptography, but the cryptographic algorithms impact the processing power and energy of these sensor nodes, where the capacity of the sensor nodes in this aspect is very limited and cost effective. The authors [36] proposed a method where the data should be anonymized before transmission to a BS and from there it will be transmitted to central server and the medical representative decides and take the decision or action towards the collected data. The cluster heads are defined to collect the data from the sensors for clustering and transmitted to BS. Later anonymity is applied with k-independent indistinguishable sensor values. The experimentation reveals that the proposed approach is applicable to all cryptographic approaches with the constraints such as energy, delays and aggregate network traffic and produced the efficient privacy mechanism with minimization of the parameters.

The heath data is collected and shared with the healthcare providers with wearable devices enhances the health services to the users. The health care data involves the personal or sensitive information and this unprotected data sharing results in privacy violation to the personal information or lead to privacy leakage problem. The traditional solution to handle this problem is differential privacy but this has several limitations in healthcare situations, because they don't use the unique parameters to collect the data from the wearable like pattern conservation and continuous real time collection. The authors proposed [37] a method to releasing the real time health data known as Re-DPoctor and this uses w-day differential privacy approach where health data collected from continuous w days is preserved to provide privacy. The utility is increased with partitioned algorithm to protect the pattern of the health data and also the adaptive techniques along with budget allocation methods are used to improve the privacy preservation of the data. The Re-DPoctor satisfies the w-day differential privacy and it is proved with the experimentation. And also, the experimental results proved that the proposed model out performs compared to the existing state of the art methods in terms of better utility and strong privacy.

To provide user identity privacy protection the authors [38] proposed dynamic and efficient ID-based authentication technique for telecare medical information systems. The authors addressed the user anonymity, disjoint relations computational load on the server side while transforming the personal or sensitive data. The users can be tracked easily by the attacker with identity guessing attack or disjoint relation attack and also the existing methods are vulnerable undetectable password guessing attack or off-line password guessing attack when the user's grid is known. To accept a legal user or discard an illegal user, it required high computational overhead at server side. The proposed approach uses the authentication system with smart cards and this smart card-based accessing will counters the problems of the existing methodologies and also improves the efficient and security of the user personal data privacy.

The health information exchange systems efficiently operate with Personal health record (PHR) service. The patients them self individually will maintain their health records in the web in PHR system, but in practical scenarios the PHR will take the help of cloud service providers for this purpose. There is a serious need to have the privacy requirement to the cloud, because cloud service may reveal the users sensitive data to PHRs and unauthorized users or other cloud service providers. The secure and more flexible access control is achieved with attribute-based encryption scheme for encrypting the patients PHRs in clouds. The authors [39] provided the flexible access control and efficient revocation with privacy –preserving PHR in cloud computing environment. The patient is connected with sensitive access tree structure with cipher text to achieve fine grained access control in PHR encryption process. Anonymous key issuing protocol is used to achieve privacy preserving in PHRs. The unauthorized users won't get anything about users GID, anonymous key issuing protocol is executing on cloud and it is very difficult to get user attributes with GID tracing. The proposed scheme assumes that multiple data owners exist and patients PHRs uses encryption for data and stored in the servers. The process overhead is minimizing with on-demand lazy user revocation method and the security of the proposed method is very high for privacy protection of sensitive information of the users.

The quality of the life is improved with the usage of next-generation healthcare systems like Mobile healthcare social networks (MHSNs), but there is various security and privacy breaches exists when transforming the personal healthcare information (PHI) to others. The authors proposed [40] scalable and fine-grained data access control to maintain the patient's full control on their PHI. The proposed model is based on the attribute-based encryption and in general the PHI sharing reveals the information about the owners or recipients. The proposed technique uses attributes contain name & value and before decryption it checks attributes efficiently with Bloom filter. Hence, the policy and data privacies are preserved with this in proposed approach. The proposed approach is outsourced for attribute-based encryption & decryption to the cloud and preventing the cloud from the reading of content and access policies with the assumption that complexity of the access policy raises the computational cost and energy & resource limitation in smart phones. The experimental results reveal that performance analysis and security of proposed approach holds the fine-grained access policies for PHI sharing. However, the proposed EPPS achieved fine-grained access control, but the hidden access policies for cloud should be easy to implement in mobile phones with constrained resources.

In the health information exchange one of the patient centric approaches is Personal health record (PHR) an it is always outsourced to the third party like cloud providers. There is a privacy concern, when the personal health care information is uncovered to the cloud servers and providing the access to unauthorized people. The encryption of the PHRs is essential while patients are accessible to other

patients PHRs before outsourcing to clouds. The authors proposed [41] a patient centric framework to address the privacy problems such as scalability in key management, flexible access, and privacy exposure and user revocation efficiently. The proposed model is to data access control to PHRs which are stored in third part servers. To attain fine-grained access control over PHRs the proposed technique adopts attribute-based encryption for encrypting patient records. The proposed approach reduces the key management complexity for users and owners by dividing the PHR users into multiple security domains because the proposed approach is focused on the multiple data owner scenario rather than individual owner. The advantage of the proposed method is it provides high degree of patient privacy by exploring the multi authority attribute-based encryption. It also supports dynamic alteration of file attributes, access policies and enables on-demand attribute or user revocation under emergency situations. The experimental results of the proposed method expose high security, scalability, and efficiency.

In [42] the authors achieved high secure and privacy-based healthcare information sharing with attribute-based authentication method and attribute-oriented transformation method for health social networks (HSNs). The proposed method provides more security to the users of HSNs for creating secure social relations with authorized or trusted users and share their health information among them. The attribute-oriented authentication method allows every HSN user to create an attribute proof for itself, where anonymized sensitive attributes are present. The users are known the attributes of other HSN users, once their attribute proof is verified. The attribute-oriented transmission method allows the user of HSN to encrypt the health information with customized access policy. The decryption of the cipher text is possible only to the users who have cleared the access policy. The experimental results with simulation study reveal that the proposed method is more secure and resist to several attacks such as attribute trackback attack, collusion attack, eavesdropping attack and forgery attack. The users also protect their own privacy, whenever the health information sharing applications reveals the personal health data. The efficiency and simplicity of the proposed approach is compatible to use with any HSN framework. The performance of the proposed framework is unstable for more complicated social environment, where the HSNs have more diversified behavior and requirements than traditional scenarios.

Providing the security for the private data in healthcare process for process mining is a challenging task for people of healthcare domain. The data mining community has been developed various techniques for privacy-preserving of data without considering the privacy issues on the data and many of these approaches are applicable for the data processing. In this [43] the authors proposed done analysis on the privacy requirements of healthcare process and evaluated the applicability of the privacy-preserving approaches to anonymize this data. The authors considered three publicly existed healthcare event logs for evaluating the influence of the existing anonymized approaches for several process mining consequences. The experimentation result reveals that the performance of the anonymization approaches differs for various process mining methods and depends on the specific data log characteristics. The proposed approach defines a framework that uses metadata and supports analysis of healthcare mining processes. It also records the historical log of privacy-preserving transformation implemented on the privacy metadata.

The possible openings offered for big data in healthcare domain such as clinical care, personal health system and drive health is unlimited and there exists various challenges that affect its original performance such as privacy & security issues, technical challenges and skilled people. The authors [43] addressed various issues related to the privacy and security in big data domain of healthcare applications. The authors evaluated the latest available and used privacy preservation on the healthcare data and validated the various anonymized methods and encryption algorithms used for protection of healthcare data along with their limitations. The reviewed techniques such as haystack, Homomorphic encryption and Attribute based encryption and storage path encryption. The authors suggested various key issues towards protecting the privacy and security in the area of bigdata for healthcare data. There is a need to enhance the privacy of approaches, because IoT is developing rapidly and the lower the performance with the greater the quantity. The quality of the data should not be affected with the privacy-preserved approaches to get the desired results [45,46]. Finally, the authors addressed the way to reconciling security and privacy prototypes with the simulation of varied methods to maintenance decision making and planning schemes.

Pros and Cons of the methods suggested for Healthcare privacy preserving

In this section, the analysis is done for security and privacy challenges in protecting personal information of healthcare data from the discussion of various existing methods and techniques for various healthcare organizations are highly beneficial in attaining privacy and security. This section presents various approaches and methodologies from different papers with the emphasis on their advantage and limitations. The limitations of various methods are consolidated as below:

- Several approaches still follow K-anonymity method but are vulnerable to correlation attack.
- The execution time of traditional approaches is affected by noise size.
- To address the unique privacy issues in big data analytics, significant research efforts required.
- Many approaches depend totally on cloud servers or cloud service provider to distribute healthcare personal information. So, if service provider is compromised the whole system fails to maintain privacy.
- Anonymization technique is used in various privacy preserving techniques, but it is vulnerable to correlation attack.
- Patient personal information and profiling can easily lead to data leakage based on revealing of sensitive

information such as age gender, ethnic background, health condition, social, background, and so on.

- Distributed cloud-based framework requires design and implement of fast and efficient privacy mechanism in order to increase cloud computation power and attain great scalability.
- The training data in IoT and Cloud environments are distributed, and every shared data portion of huge volume cannot attain distributed feature selection.
- Many are using cryptographic functions but the trust level in the cryptographic server is limited.

CONCLUSION

This manuscript summarizes the state-of-the-art Privacy Preservation techniques proposed in different areas like Surveillance, Health care, e- commerce and electronic and social media related data publication along with the pros and cons which gives motivation to work on different areas like surveillance and health care data publication without violating the personal privacy of the individuals with better utility functionality. The subsequent work proposes different policies to publish data and compared with the existing state of the art methods toimprove accuracy, efficiency, utility and privacy tradeoffs in different areas.

REFERENCES

[1] Kuan-Yu Chu, et.al. 2013. Real-time privacy-preserving moving object detection in the cloud. In Proceedings of the ACM Conference on Multimedia. 597–600.
[2] H. Sohn, et.al. Privacy-preserving watch list screening in video surveillance system. In PCM (1), pages 622–632, 2010.
[3] ZekeriyaErkin, et.al. 2009. Privacy preserving face recognition. In Privacy Enhancing Technologies. Springer, 235–253.
[4] Chris Poppe, et.al. 2009. Moving object detection in the H.264/AVC compressed domain for video surveillance applications. J. Visual Commun. Image Represent. 20, 6 (2009), 428–437.
[5] Christopher Thompson and David Wagner. 2016. Securing recognizers for rich video applications. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, 53–62.
[6] M. Upmanyu, et.al. Efficient privacy preserving video surveillance. In ICCV, pages 1639–1646, 2009.
[7] S. Jana, et.al. Protecting user privacy from perceptual applications. In Proceedings of the 34th IEEE Symposium on Security and Privacy, 2013.
[8] Lee, Donghyeok& Park, Namje. (2020). Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimedia Tools and Applications. 10.1007/s11042-020-08776-y.
[9] Gallo P, Pongnumkul S, Nguyen UQ (2018) BlockSee: Blockchain for IoT video surveillance in smart cities. In: 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). IEEE
[10] Mendki P (2019) Blockchain enabled IoT edge computing. In: Proceedings of the 2019 International Conference on Blockchain Technology. ACM
[11] Jeong Y, Hwang DY, and Kim K-H "Blockchain-based management of video surveillance systems. 2019 International Conference on Information Networking (ICOIN). IEEE, 2019.
[12] Costin, "Security of CCTV and video surveillance systems: threats, vulnerabilities, attacks, and mitigations," in Proceedings of the 6th International Workshop on Trustworthy Embedded Devices. ACM, 2016, pp. 45–54
[13] Xiaojing Ma et.al. "Efficient Privacy-Preserving Motion Detection for HEVC Compressed Video in Cloud Video Surveillance" , 2018 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS): BigSecurity 18: The Fourth International Workshop on Security and Privacy in Big Data,2018.
[14] H. Du, et.al. A System for Privacy-Preserving Cloud Video Surveillance," in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1252-1261, June 2020, doi: 10.1109/JSAC.2020.2986665.
[15] M. Saini, et.al. "Adaptive transformation for robust privacy protection in video surveillance," Adv. Multimedia, vol. 2012, May 2012, Art. no. 639649.
[16] Bentafat E., Rathore M.M., Bakiras S. (2020) A Practical System for Privacy-Preserving Video Surveillance. In: Conti M., Zhou J., Casalicchio E., Spognardi A. (eds) Applied Cryptography and Network Security. ACNS 2020. Lecture Notes in Computer Science, vol 12147. Springer, Cham. https://doi.org/10.1007/978-3-030-57878-7_2.
[17] PavelKorshunov, ShutingCai, and TouradjEbrahimi. 2012. Crowdsourcing approach for evaluation of privacy filters in video surveillance. In Proceedings of the ACM multimedia 2012 workshop on Crowdsourcing for multimedia (CrowdMM '12). Association for Computing Machinery, New York, NY, USA, 35–40. DOI: https://doi.org/10.1145/2390803.2390817
[18] M. Usman, M. A. Jan, X. He and J. Chen, "P2DCA: A Privacy-Preserving-Based Data Collection and Analysis Framework for IoMT Applications," in *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1222-1230, June 2019, doi: 10.1109/JSAC.2019.2904349.
[19] Zhenyu Wu, et.al. "Privacy-Preserving Deep Action Recognition: An Adversarial Learning Framework and A New Dataset", IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2 Oct 2020.
[20] Fitwi and Y. Chen, "Privacy-Preserving Selective Video Surveillance," *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, Honolulu, HI, USA, 2020, pp. 1-10, doi: 10.1109/ICCCN49398.2020.9209688.
[21] Pascal Birnstill, et.al. Privacy-preserving surveillance: an interdisciplinary approach, *International Data Privacy Law*, Volume 5, Issue 4, November 2015, Pages 298–308, https://doi.org/10.1093/idpl/ipv021.
[22] Nakashima, et.al. (2010). Development of privacy-preserving sensor for person detection. Procedia - Social and Behavioral Sciences. 2. 213-217. 10.1016/j.sbspro.2010.01.038.
[23] Rajpoot Q.M., Jensen C.D. (2014) Security and Privacy in Video Surveillance: Requirements and Challenges. In: Cuppens-Boulahia N., et.al. (eds) ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_14.
[24] AnastasiiaPika , et.al. "Privacy-Preserving Process Mining in Healthcare", Int. J. Environ. Res. Public Health 2020, 17, 1612; doi:10.3390/ijerph17051612.
[25] Pika, A, et.al. Towards Privacy-Preserving Process Mining in Healthcare. In Business Process Management Workshops, Proceedings of the International Workshop on Process-Oriented Data Science for Healthcare Vienna, Austria, 1–6 September 2019; Springer: Cham, Switzerland, 2019; LNBIP 362, pp. 483–495.
[26] W. Tang, J. Ren and Y. Zhang, "Enabling Trusted and Privacy-Preserving Healthcare Services in Social Media Health Networks," in IEEE Transactions on Multimedia, vol. 21, no. 3, pp. 579-590, March 2019, doi: 10.1109/TMM.2018.2889934.
[27] Miyaji, A., Nakasho, K. & Nishida, S. Privacy-Preserving Integration of Medical Data. J Med Syst 41, 37 (2017). https://doi.org/10.1007/s10916-016-0657-4.
[28] E. Luo, et.al. "Privacy protector: Privacy-protected patient data collection in IoT-based healthcare systems", IEEE Commun. Mag., vol. 56, no. 2, pp. 163-168, Feb. 2018.
[29] H. Tao, et.al. "Secured data collection with hardware-based ciphers for IoT-based healthcare", IEEE Internet Things J., vol. 6, no. 1, pp. 410-420, Feb. 2018.
[30] W. Tang, et.al. "Lightweight and privacy-preserving fog-assisted information sharing scheme for health big data," in Proc. of IEEE GLOBECOM, 2017, pp. 1–6
[31] W. Meng, et.al. "Towards bayesian-based trust management for insider attacks in healthcare software-defined networks," IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 761–773, 2018.
[32] L. Zhang, et.al. "Privacy protection for ehealth systems by means of dynamic authentication and three-factor key agreement," IEEE Transactions on Industrial Electronics, vol. 65, no. 3, pp. 2795–2805, 2018.

[33] X. L. Li, et.al. "Secure Privacy-Preserving Biometric Authentication Scheme for Telecare Medicine Information Systems," Journal of Medical Systems, vol. 38, p. 8, Nov 2014.
[34] M. Barua, et.al. "SPS: Secure personal health information sharing with patient-centric access control in cloud computing," in Proc. of GLOBECOM, 2013, pp. 647–652.
[35] P. Belsis and G. Pantziou, "A k-Anonymity Privacy-Preserving Approach in Wireless Medical Monitoring Environments," J. Personal Ubiquitous Comp., vol. 18, no. 1, 2014, p. 6174.
[36] J. Zhang, et.al. "Re-DPoctor: Real-Time Health Data Releasing with W-Day Differential Privacy," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8254014.
[37] Cao, T., and Zhai, J., Improved dynamic ID-based authentication scheme for telecare medical information systems. J. Med. Syst. 37(2):1–7, 2013.
[38] Qian, H., Li, J., Zhang, Y. et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. Int. J. Inf. Secur. 14, 487–497 (2015). https://doi.org/10.1007/s10207-014-0270-9
[39] Jiang, S.; Zhu, X.; Wang, L. EPPS: Efficient and Privacy-Preserving Personal Health Information Sharing in Mobile Healthcare Social Networks. *Sensors* 2015, *15*, 22419-22438.
[40] Li, M.; Yu, S.; Ren, K.; Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. 2013, 24, 131–143.
[41] Liang, Xet.al. Achieving secure and privacy-preserving health information sharing through health social networks. Comput. Commun. 2012, 35, 1910–1920.
[42] AnastasiiaPika, et.al. "Privacy-Preserving Process Mining in Healthcare", Int. J. Environ. Res. Public Health 2020, 17, 1612; doi:10.3390/ijerph17051612.
[43] Abouelmehdi, et.al. Big healthcare data: preserving security and privacy. J Big Data 5, 1 (2018). https://doi.org/10.1186/s40537-017-0110-7.
[44] Standards for privacy of individually identifiable health information. Final Rule, 45 CFR parts 160 and 164. http://www.hhs.gov/ocr/privacy/hipaa/administrative/ privacyrule/adminsimpregtext.pdf (accessed 20 Feb 2012).
[45] Pavan Kumar Vadrevu, et.al. Personal privacy preserving data publication: Ɛ- Differential privacy perspective, Solid State Technology, Volume: 63 Issue: 5 Publication Year: 2020.
[46] Pavan Kumar Vadrevu, et.al. A hybrid approach for personal differential privacy preservation in homogeneous and heterogeneous health data sharing, High Technology Letters Volume 26, Issue 9, 2020 ISSN NO: 1006-6748.