JOURNAL OF DYNAMICS AND CONTROL

VOLUME 8 ISSUE 9

ENSURING MEDICAL RESEARCH QUICK PROTECTION THROUGH DIGITAL TIMESTAMPING

Saima Zareen Ansari, Dr. Shrikant D. Zade

G.H. Raisoni University, Saikheda, M.P., India

ENSURING MEDICAL RESEARCH QUICK PROTECTION THROUGH DIGITAL TIMESTAMPING

Saima Zareen Ansari[1], Dr. Shrikant D. Zade[2]
G.H. Raisoni University, Saikheda, M.P., India
[1]saimaansari16@gmail.com, [2]cdzshrikant@gmail.com

ABSTRACT: Medical research has been grown in many ways and the fact it is not limited to research labs only. Different observations and results could be concluded after communication with multiple patients and this is the simplest form of research. Not only the doctors and researchers, but even the pathology laboratory experts could also involve in medical research as they might deal with actual observations. The terminology is on any medical research multiple volunteers may get involve and research may go through multiple stages with different levels of conclusions and results. Major problems lie here when research gets completed the possible intellectual shares are equal to everyone in the team where everyone may have different and low or high-value inputs. IP protection won't give any direct solutions on paper, and it has to handle mutually between every team member. Since IP protection process is lengthy, complex, and time taking process not everyone willing to involve into process but avoiding result into IP loss. Digital timestamping could solve the problem of quick IP protection and utilizing for future IP argument claims proof. Proposed research work primarily focuses on utilizing the digital timestamping mechanism for quick protection and future proof of medical research ownership.

KEYWORDS: IPR, Digital Timestamp, Blockchain.

I. INTRODUCTION

Intellectual Property (IP) protection is most critical to advancing improvement. Without protection of every novel idea, individuals and the businesses would not gain the full and deserved benefits of their innovative work and would emphasis less on novel research and development. In medical research, intermediate results are as valuable as the final outcome. So, the protection of intermediate results also needs the same attention. On other hand digital timestamping or Bern conventions are acceptable at different countries for quick protection of the data and this time protected data could be used for future ownership and first to present claims. In IP protection, time of the presented idea is most important factor and considered as a first to present become owner of data model. In many cases presenting partial information could be important but presenting for IP protection is not valid hence partial data also need quick protection before presenting as final result.

An encoded sequence of characters, or timestamp, is used to determine the exact time and date of an occurrence. It can sometimes be precise to within a few microseconds of the actual time. However, timestamps don't have to be based on a rigid interpretation of time. They can be associated with any era, with any arbitrarily chosen time (e.g., the system power-on time), or with any arbitrarily chosen historical point. Depth of time description may changes as per the requirement or the demand of the implementing system like data presentation may till second, millisecond, or the microsecond level accurate or categorized.

Digital timestamping and securing the data is best quick method for IP protection and first to present owner of data claim. In digital timestamping secured data can be only delete or read by registering authorities or owner and not even owner of data can edit the data or its timestamp. Hence this data timestamping method could make the data secure and presentable for future use including the proof of existing of data from the mentioned timestamp. Our aim is to implement a de-centralized security mechanism for protecting different stages of research having sequential interlinked individual records/intermediate results. The proposed system is aimed to address main issues which need strong research ownership protection mechanism using standardized data design and its deployment using Blockchain or other secured distributed Technologies. This way we can give every medical researcher the right and platform to quick protect their research or novel work and use it in future to prove its existence before time.

II. BACKGROUND

Trusted Digital Timestamping

The process of safely keeping track of the creation and later modification times of each secured document is known as digitally trustworthy timestamping. The notion of security in this context clearly means that once data is documented, nobody, not even the data owner, should be able to alter it, and that the validity of the digital timestamping authority will never be called into question. The administrative part entails putting in place a reliable, publicly accessible timestamp management system in order to gather, handle, and renew timestamps.

The Time Stamping Authority (TSA) or the trustworthy Third Party (TTP) issues and provides a safe and a trustworthy digital timestamp for document security in accordance with the RFC with reference number 3161 standards. After that, it's used to demonstrate the existence of particular data on or before a given date (such as contracts, medical records, and research records) without allowing the owner to alter or retroactively date the timestamps. Utilizing several time stamping authorities can increase dependability and prevent vulnerabilities. In addition to a legitimate time source that can be verified by any third party, the RFC reference number 3161 standard describes documents-level security criteria to verify data validity in the updated ANSI-ASC-X9.96 Standards for trustworthy timestamping methods. Digitally encrypted and signed data has been verified using this standard for financial transactions, regulatory compliance, and legal purposes.

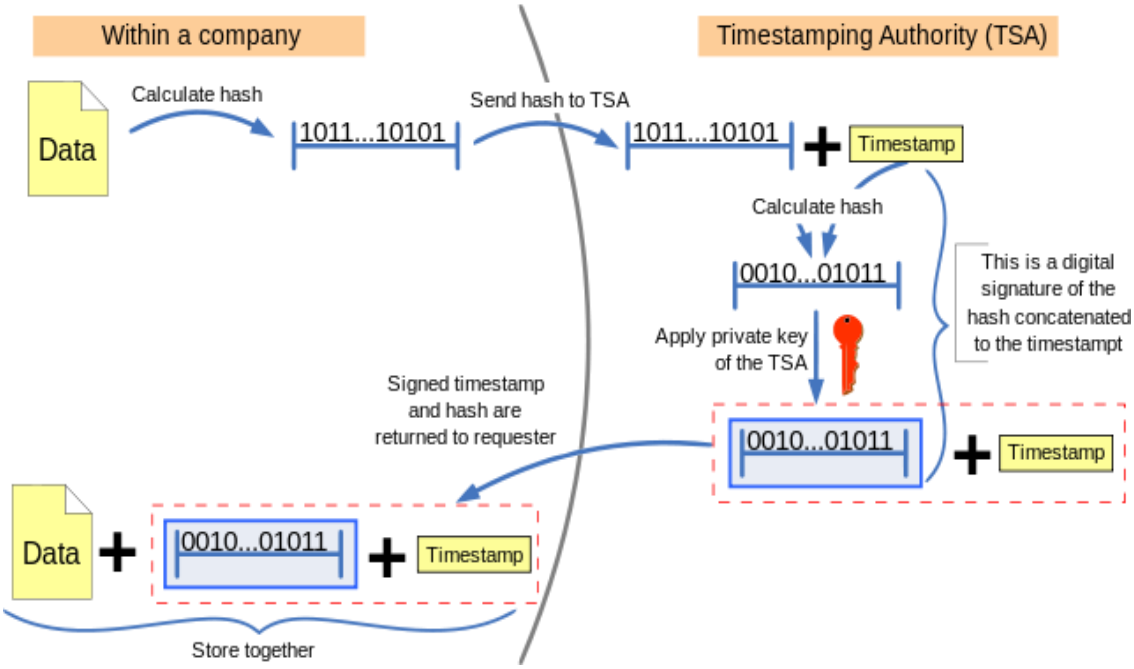

Figure 1.0: Digital timestamping workflow

Creating a digital timestamp

Digital signatures and hash functions serve as the foundation for digital timestamping technologies. Determine the hash value first using the data. A hash is a string of bits that is nearly impossible to duplicate with another collection of data, thus serving as a digital fingerprint of unprocessed data. A totally new hash would result from altering the original data. The TSA receives this hash. TSA computes this concatenated hash by appending the timestamp to the hash. Afterward, the TSA's private key is used to digitally sign this hash. The timestamp seeker receives this signed hash + timestamp back and stores it alongside the actual data (see diagram). This method is acceptable for classified material because the TSA can never see the original data because it is impossible to calculate from the hash (because the hash function is one-way).

Checking the timestamp

The document was not created after the date the time-stamper attests to, which anyone who believes the time-stamper may confirm. Furthermore, the claim that the person who requested the timestamp was in possession of

the original material at the moment the timestamp was provided cannot be refuted. This is demonstrated (see figure) by first computing the hash of the original data, adding the timestamp provided by the TSA, and then computing the hash of the concatenated result. This hash is called ‘A’.

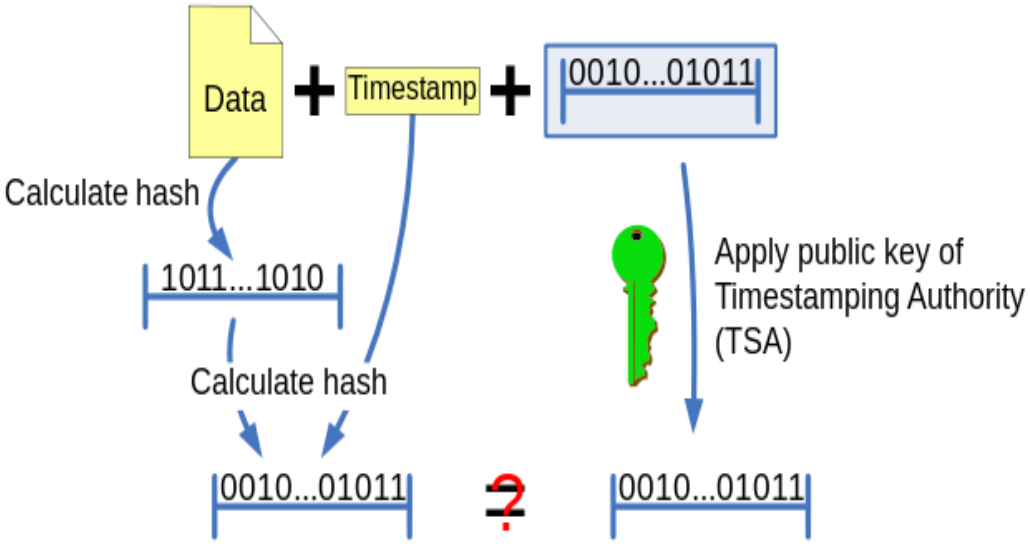

Figure 2.0: Checking the timestamp

Next, the TSA's digital signature needs to be verified. This is accomplished by generating hash ‘B’ by decrypting the digital signature using the TSA public key. The timestamp and message are shown to be authentic and to have been provided by the TSA when hash 'A' and hash 'B' within the signed TSA message are compared to verify they are equal. If not, the timestamp was either not provided by the TSA or it was changed. The timestamp was issued by the TTP and neither the document nor the timestamp were altered if the computed hash-code matches the outcome of the decoded signature. If not, then neither of the earlier claims is accurate.

Distributed timekeeping using blockchain

It is now possible to obtain a certain degree of safe timestamp accuracy in a decentralized, tamper-proof manner thanks to the introduction of cryptocurrencies like bitcoin. It is possible to hash digital data and then incorporate that hash into a blockchain transaction to provide proof of the data's existence at a specific time. The security of proof-of-work blockchains comes from the massive amount of computation that is done once the hash is added to the blockchain. It would take more computing power than the entire network to tamper with the timestamp, and in an actively guarded blockchain, such an attempt would be detected.

However, because of the way Bitcoin is implemented and designed, timestamps can be manipulated to some extent. New blocks that have timestamps earlier than the preceding block can be accepted, and timestamps can be set up to be up to two hours in the future. The blockchain-based decentralized timestamping technique has also found use in other contexts, such dashboard cameras, where it is used to guarantee the integrity of video files at the moment of recording or to give innovative content and ideas published on social media platforms precedence.

III. PROPOSED SYSTEM

The main idea behind the proposed area of research is to standardization of the medical research records data protection and preventing the medical field research ownership to actual researcher and helping to get right credit to every inventor.

In medical field research may hold multiple module and phases where percentage of credit may matter. Major lacking in IPR, every inventor holds the same right over the invention despite of individual involvement and the role. Few results may be important for complete research and need quick protection with digital timestamping and blockchain based secure file management system.

As the EMR has multiple sources, the EMR also having multiple types starts from multi-column records to graphs or the medical imaging, hence it needs right architecture of data management or generic type data structure. Managing records is not the only issues, protecting data with read only mode with decentralization is biggest challenge. Another issue is claiming the ownership or claiming the intellectual property rights of on-going medical research is become challenging as medical research may take long time to get desired result with novel ideas or the methods.

We proposed a complete medical research data specific IP protection and secure data management generated at multiple level of medical practices. This data will be of multiple type and at multiple level. It includes centralized authentication data set and decentralizes secure file management. This ensures a quick authentication, data validation, digital timestamping to records or file and securing files over blockchain managed central storage.

In the way to achieve the objectives, architecture has been proposed where the sub-blocks are concerned for the preservation of various intermediate outcomes. A complete research work consists of multiple steps or multiple phases, where every phase contains a proper data set with the proper outcome. Proposed architecture is illustrated (See Figure 3.0).

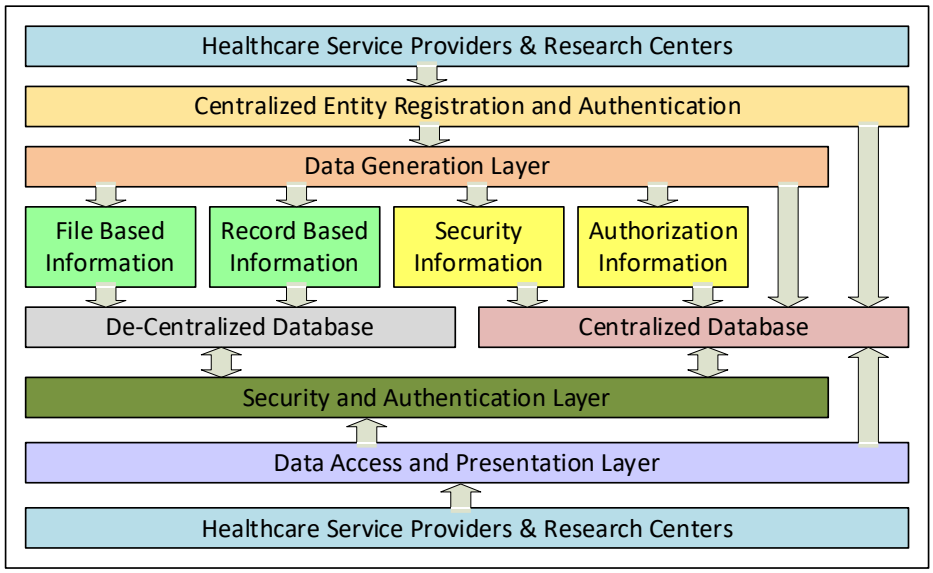

Figure 3.0: Proposed System Architecture

The complete proposed architecture covers a different aspect of the implementation and the different layers involved in the process. Those individual components are discussed as following.

1) **User base:** Since the targeted audience or the user of the systems are targeted to be healthcare related person, hence primarily employees from healthcare service provider and the research group and research centers of the healthcare industries will be the primary user of the proposed system.
2) **Registration and authorization:** Every user has to be registered and authorized to access the features or the functionality of the system. This authorization and registration process will be secured using secure digital certificate system.
3) **Database structure:** In order to manage the records and the documents there will be separate model will be adopted. For all security authentication and verification information will be stored on centralized data base server and other information like user documents and information will be managed and stored on de-centralized database server. There will be four different type of record set or the information.
    a) File based dataset to store the document and images.
    b) Record based dataset to stored user literatures and the articles.
    c) Security dataset to hold individual users profile information.
    d) Authorization dataset to store user authentication security information.

4) **Data generation and accessing layer:** These two layers are primarily used to generate the information by creating or writing the documents and upload it to central server. System will be having some text editor's functionality to write down the articles or the notes and the document upload, download functionality to manage documents on-line or centrally. These same records or the documents are then could be presented or authenticated as per the demand or the requirement of the system. This will be handled by information retravel model and user interface.

System Workflow

Proposed system workflow has multiple micro components involved for successful implementation those are clearly described in figure 4.0 and stages are explained as follows,

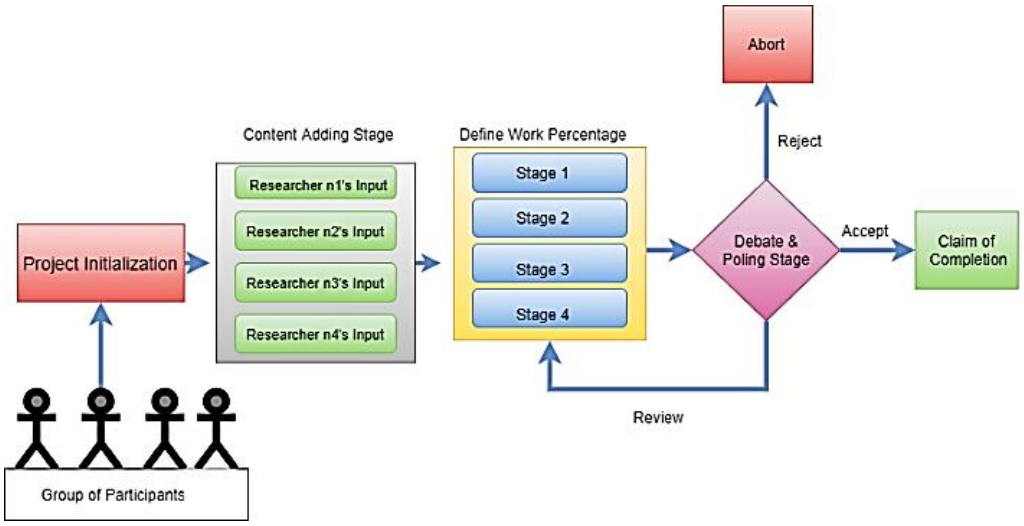

Figure 4.0: Proposed System Workflow

Stage 1: Registration of Individual Members

The first step involves the registration of each individual member in the IPR office portal. This process requires the user to have a valid digital signature, which serves as a unique identifier ensuring the authenticity and security of their identity. The digital signature is essential for accessing the portal, submitting documents, and performing other actions securely. The portal can verify that a user is authentic by employing a digital signature, which lowers the possibility of unwanted access and guarantees that all acts made on the portal can be tracked down and verified.

Stage 2: Formation of a Group

Forming a group of people to work together on a particular topic or idea comes after individual registration. At this point, a list of all the participants and thorough project details must be provided. An in-depth explanation of the innovation, the goals, and the responsibilities of each participant should all be included in the project specifics. This methodical technique guarantees that each member's input is recorded right away, promoting open communication and teamwork among the members.

Stage 3: Document Submission and Timestamping

It is the duty of each group member to upload pertinent documents to the group portal. Timestamped documents guarantee that the intellectual property contributions are recorded in a verifiable way by capturing the precise moment of submission. A document is visible to every group member as soon as it is uploaded. After then, a polling method is employed so that participants can assess the work that has been provided and offer their approval or criticism. By establishing the worth of each member's contribution through collaboration, this review method promotes an open and democratic approach to project development.

Stage 4: Agreement and Finalization

Once everyone has agreed upon the contributions, the group must formally announce their agreement. This entails determining the worth or percentage of each team member's contribution to the project and recording it. The parameters of the collaboration and the division of intellectual property rights must be agreed upon by all members. This agreement is essential to averting future conflicts and guaranteeing that each member's contribution is appropriately acknowledged and valued. When the agreement is complete, it is included with the project records.

Stage 5: Submission for IPR Examination

The last step is submitting the entire project to the IPR authority for review and examination. This entails sending all pertinent agreements, papers, and other required information to the IPR office. The authority will then review the submission to make sure it satisfies all requirements and standards for the protection of intellectual property rights; this may entail additional review, comments, or requests for information from the IPR office. If this step is completed successfully, the intellectual property will be formally recognized and protected, giving the group legal rights and protection for their innovation.

By following these detailed stages, individuals and groups can systematically manage their intellectual property, ensuring that their innovations are protected and that all contributions are fairly recognized.

Since the proposed system is in generic nature so it can be implemented for multiple types of IPR (Intellectual Property Rights) protection. One of the modules titled digital timestamping in proposed system can be used for protection of any document or the article. Financial issues and dispute in IPR can be addressed before the issues raised or generated. The only challenge in this process is required and driven by government authority on the continent. This project deployment and the implementation need a higher authority's involvement and the acceptance to make it working in public domain.

IV. IMPLEMENTATION

In Implementation process there are three major role players involved and holding different authorities those are a) user requesting and accessing the digital timestamping service, b) Centralized authority to deal with user request and management of user validation, authentications, and requests, c) Digital timestamping server which holds actual timestamped file records and issues the digital timestamping server.

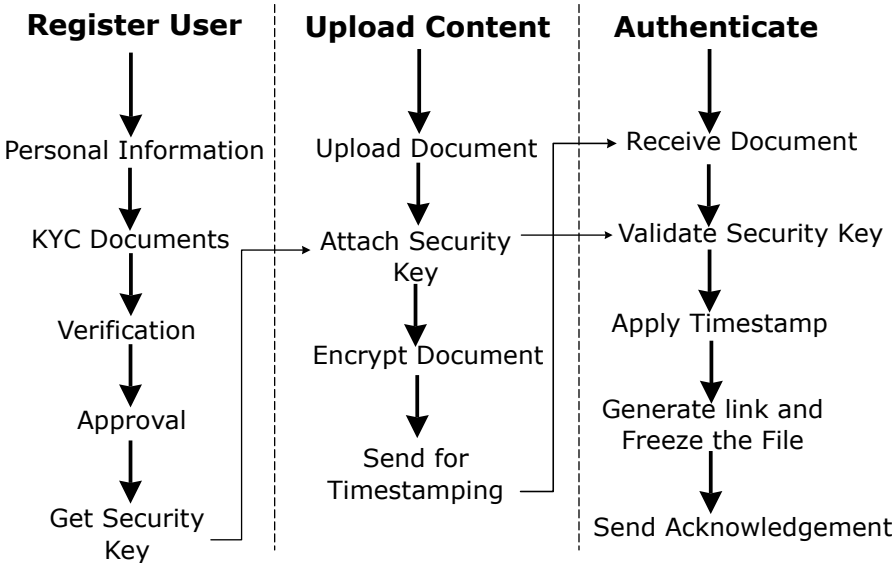

Figure 5.0: Timestamping based file management and validation process

To issue timestamping digital certificate and protect records user need to go through multiple stages of registration, authentication, file management and digital certificate management as described in figure 5.0. After successful registration and authentication user will get the access to digital timestamp server file management application and a user private digital signature. Before uploading any new document to digital time stamp server user need to encrypt or apply hash to document using private digital signature. This will ensure user ownership to uploaded document. Further protecting and storing document with digital time stamp will be management by digital timestamping services.

Starting with the user registration procedure, which requires all users, members, and IPR application groups, including inventors and applicants, to register on the system by supplying personal information and KYC papers for identity verification, document protection will begin. The suggested system would generate a unique secret key, also known as a private key, for each individual user when the verification procedure is successfully completed, and the application is approved to become a member. The user will then receive the key from. The user must carry this key in the form of a file or notes, and he must keep it safe and secure.

The user's security of the document is the second step in the process. In order to do this, the user must log in to the portal and upload the original, owned file to the server. The user must attach the security key that they got during the registration process after uploading. After the security key has been assigned, the user can secure the document by encrypting it and sending it for the last stage of timestamping.

Following the upload of documents for time-tagging protection, an authentication process is initiated. A digital timestamp server receives the user document and uses a centralized user database to validate its security key. After the security key is verified, the server applies the digital timestamp to the file, stores it in a secure location, and creates an external file access link with a unique serial number for each uploaded file. Every file's ownership metadata is likewise managed by the server. The file link with the serial number is sent by the server after the timestamping process is finished, acknowledging that the timestamping and secure protection were successful.

V. CONCLUSION

Which documents would benefit from digital timestamping that is secure? Timestamping has a clear purpose for records that prove an innovation or concept came before them. Digital timestamping's ability to establish intellectual property precedence without revealing its contents is a particularly useful characteristic. This might be applied to anything from software to the Coca-Cola recipe, and it could have a big impact on copyright and patent law. But what about documents where the question of whether or not they have been altered trumps the significance of the date? In the following situations, timestamping these documents can also be beneficial. Let's say it can be demonstrated that either the required information or the incentive to alter a document did not exist until far later. Consider a business that processes a lot of documents every day, a small percentage of which are subsequently discovered to be incriminating. If every document created by the corporation had a time stamp applied to it at the moment of creation, it would be too late to alter any of the documents by the time it became clear which ones were implicating and how to change them. Such documents are known as tamper unpredictable. It appears that many company documents are susceptible to tampering. Thus, many documents' credibility may be increased if timestamping were added to the standard operating procedure. A variant that could be especially helpful for business documents is to timestamp a collection of documents as opposed to each one separately. One possible application of this would be to hash every business document that is created in a given day and add the hash value to the company's daily record of documents. The log by itself could then be submitted for timestamping at the conclusion of the business day. In addition to avoiding the cost of time-stamping each document separately, this would allow us to detect any tampering with the documents and identify any that have been destroyed. Digital timestamping is, of course, not exclusive to text documents. Time-stamped files can be created from any sequence of bits, including full-motion films, digital audio recordings, and photos. Most of these documents are susceptible to tampering. Timestamping, thus, can assist in differentiating between an original photograph and one that has been altered, a problem that has recently drawn a lot of attention from the public publications. Actually, it's hard to imagine another algorithmic "fix" that could give photos, movies, or audio recordings greater legitimacy than timestamping.

VI. REFERENCES

[1]. Lu, L., Zhang, C., Liu, Y., Zhang, W., & Xia, Y. (2019). IEEE 1588-Based General and Precise Time Synchronization Method for Multiple Sensors*. 2019 IEEE International Conference on Robotics and Biomimetics (ROBIO). doi:10.1109 /robio 49542. 2019. 8961658

[2]. 10 Benefits and Challenges of Blockchain Technology in Healthcare. https://seeromega.com/10-benefits-challenges-blockchain-technology-healthcare/ Accessed: 2021-04-24.

[3]. 25+ Blockchain companies in healthcare to know|2017 https://www. beckershospitalreview. Com /lists/25-blockchain-companies-in-healthcare-to-know-2017.html. Accessed:2021-04-25.

[4]. Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O. Y., Bashir, A. K., & Abd El-Latif, A. A. (2020). DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access*, *8*, 111223-111238.

[5]. Alruwaili, F. F. (2020). Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records. *PeerJ Computer Science*, *6*, e323.

[6]. Aujla, G. S., & Jindal, A. (2020). A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. *IEEE Journal on Selected Areas in Communications*.

[7]. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)* (pp. 25-30). IEEE.

[8]. Ballantyne, A. (2020). How should we think about clinical data ownership? *Journal of Medical Ethics*, *46*(5), 289–294. https://doi.org/10.1136/medethics-2018-105340

[9]. Blockchain healthcare use cases| Blockchain in healthcare use cases https://www.leewayhertz.com/blockchain-in-healthcare/ Accessed:2021-04-25.

[10]. Blockchain Security: Is Blockchain Really Secure? | Edureka https://www.edureka.co/blog/blockchain-security/ , Accessed: 2021-05-01.

[11]. Cyber security, https:// www. who.int/ about/ communications/cyber-security, Accessed: 2021-05-01.

[12]. Du, X., Chen, B., Ma, M., & Zhang, Y. (2021). Research on the Application of Blockchain in Smart Healthcare: Constructing a Hierarchical Framework. *Journal of Healthcare Engineering*, *2021*.

[13]. Fernandes, A., Rocha, V., da Conceição, A. F., & Horita, F. (2020, March). Scalable Architecture for sharing EHR using the Hyperledger Blockchain. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)* (pp. 130-138). IEEE.

[14]. Gong, J., & Zhao, L. (2020). Blockchain application in healthcare service mode based on Health Data Bank. *Frontiers of engineering management*, *7*(4), 605-614.

[15]. Gupta, M., Kumar, V., Yadav, V., Singh, R. K., & Sadim, M. (2021). Proposed Framework for Dealing COVID-19 Pandemic Using Blockchain Technology. *Journal of Scientific and Industrial Research (JSIR)*, *80*(03), 270-275.