General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management

Nasr Al-Zaben
Department of Computer Engineering
Inje University
Gimhae, Korea
nasr.zaben@hotmail.com

Md Mehedi Hassan Onik
Department of Computer Engineering
Inje University
Gimhae, Korea
hassan@oasis.inje.ac.kr

Jinhong Yang
Department of Healthcare and IT
Inje University
Gimhae, Korea
jinhong@inje.ac.kr

Nam-Yong Lee
Department of Applied Mathematics
Inje University
Gimhae, Korea
nylee@inje.ac.kr

Chul-Soo Kim
Department of Computer Engineering
Inje University
Gimhae, South Korea
charles@inje.ac.kr

Abstract— **Surveillance and secrecy breaching incidents of users' privacy questioned the current third-parties data collection procedure. Massive amounts of Personally Identifiable Information (PII) are being exploited due to malpractice, identity theft, spamming, phishing and cyber-espionage. A large amount of data flow from users to enterprises for data-driven market analysis and prediction. Consequently, it is tough to track the flow and genuineness of PII. Blockchain technology, an 'immutable' distributed ledger which can efficaciously track PII exchange, store, and distribution. In contrast, ongoing EU General Data Protection Regulation (GDPR) demands 'right to forget' and 'should be erasable' rights. However, this paper proposes an off-chain Blockchain architecture which uses both local database and distributed ledgers to preserve a trustable PII life cycle. Considering the key factors of GDPR, prevailing Blockchain architecture were modified and a prototype was created to validate our proposed architecture using multichain 2.0. Proposed architecture stores PII and Non-PII physically separated location. Finally, with proposed architecture user will realm privacy and rigidity of Blockchain along with the privacy regulation of GDPR. Validation is done by comparing proposed system with existing methodology from technical aspects, future research scopes is also well advocated.**

Keywords—Blockchain, General Data Protection Regulation (EU-GDPR), Personally Identifiable Information (PII), Privacy Policy, Personal data, Data Protection, Distributed ledger, off-chain Blockchain, Privacy issues, Identity management

I. INTRODUCTION

For providing user centric services, websites gather noticeable amount of Personally Identifiable Information (PII) (e.g age, race, social security numbers, house location, driving license etc.). Currently, over 50 million people use several Social Networking Sites (SNS) and have made available a vast amount of PII on these sites. All these SNS sites, other websites and mobile applications offer sign in or registration for premium services. PII are often utilized by organizations to authenticate a customer's identity. Since most of these SNS sites and applications are for free, several studies found PII breaching by these organizations. Actually, these organizations store, distribute, analyse sensitive PII information in order to generate business model through user profiling. Tech giants uses third party service providing enterprises to mine those customers PII. Ultimately, those subsidiary organizations collect, analyze and distribute data from several organization. Eventually, users are having no clue where their data are ending up with. We all are reaping the advantages of data-driven industry but the dark side is illicit use of those PII. Guardian reveals on April 2018 that, the largest SNS site Facebook breached 87 million personal information and PII of its user [1]. Constant data breaching incidents are happening in the era of big data those were mentioned by several studies [2-4]. According to Armerding [4], data breaches by different organization in 21st century are Yahoo (3 billion), ebay (145 million), Adobe (38 million), JP Morgan (76 million), US Office of Personnel Management (22 million). Gemalto's Breach Level Index (BLI) reported, out of 10. 4 million yearly PII leaking, 74% were identity stealing [5]. Forbes magazine [6] stated data as new currency in trade marketing. The reported that around 200 billion USD are being invested in order to exchange PII. Companies are exchanging their customer's data to make profit. Business to business communication will be even extensive in the era of industry 4.0 which lead us to this think about PII management and tracking.

Blockchain technology has gained much attention from several researchers and using Blockchain technology beyond cryptocurrencies [7-8]. Blockchain is constructed as a sequence of blocks, which can hold any data in its block like a conventional public ledger, which these blocks are linked and secured together using cryptography. Several other researcher has also used Blockchain in PII management [9-13]. However, the motivation of recently executed General Data Protection Regulation (GDPR) [14] is to protect individual's information therefore, institutions must pay special attention to both Individual's consent and data-sharing. Consent needs to be obtained before any private data is being analyzed, there is also accountability to confirm that this data can be withdrawn or deleted independently (aka 'the right to be forgotten'). Blockchains PII storing architecture is based on 'immutability' of the data. On contrary, General GDPR [14] demands any personal information should be mutable and erasable according to data owner's request.

This study proposes a Blockchain based Personally Identifiable Information Management System (BcPIIMS) designed for PII management throughout organizations. A separate procedure of storing PII and rest of the data is proposed. In this study, the PII is saved in local database and

Institute for Information & communications Technology Promotion (IITP) Grant No.2018-0-00261 from Korea Govt. Ministry of Science and ICT

978-1-5386-4904-6/18/$31.00 ©2018 IEEE

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on April 16,2022 at 19:26:38 UTC from IEEE Xplore. Restrictions apply.

non-PII with hash of PII is stored in Blockchain. A porotype is developed to validate the performance of proposed model. Future scope, research direction is also mentioned to create awareness in regards of PII management. In one side, proposal provides a transparent, immutable system using Blockchain technology another side, separately stored PII in local database can also be deleted at any time. As a result, Proposed Blockchain based Personally Identifiable Information Management System (BcPIIMS) comply GDPR.

Roadmap: Section II elaborates related studies. Section III discusses proposed BcPIIMS system on tracking and securing PII. Elaboration and detail description with scenarios are mentioned in that section. In section IV description of developed prototype using proposed BcPIIMS is mentioned with necessary discussion. Future work and limitations are discussed in conclusion.

II. RELATED WORKS

Several solutions and regulations are there in order to secure and track PII. To protect the privacy leading countries and big companies started to implement their own rules. A software level proprietary verification works on OAuth protocol has been proposed too [15]. Against aforementioned issues, several researchers have worked either to reduce PII breach or to track the flow of users PII [16-19]. Weingärtner [17] followed data mining technique to identity the risk factors of PII. Brill [18] identified three main factors for big data end user privacy leaking they are a) risk of information leaking in cloud b) data leaking due to gathering of more information than actually needed c) data leaking due to data distribution for analytics. Alduaij [19] analyzed several identity management techniques mostly based on privacy regulations. Several regulations like General Data Protection Regulation (GDPR) [14], Privacy Protection amendment by Australian govt. [20], Canadas Personal Information Protection [21], ISO27001 by International Standardize Organization [22] are practiced to protect or manage data flow. In privacy, several studies have identified digital identities as a source of the user identifier. Pfitzmann and Hansen [23] defined PII as “An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons”. National Institute of Standards and Technology (NIST) [24] defines PII "any information about an individual maintained by an agency, including (PII) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (linked PII or PPII) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information". Few PII are listed in Table. I

TABLE I. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII)
Full Name, Home or Office Address, Email, National Identification Number, Passport, Vehicle ID, Driving License, Fingerprints, Handwriting, Credit Card Numbers, Digital Identity, Birth date, Birthplace, Biological Information, Phone Number, Login Name, Social Security Number (SSN).

The growth of security breaches related to PII has led to the breach of millions of information in last few years. PII risks are dangerous to both organizations and individuals [25]. Privacy by design was mentioned by few studies [26-27] in order to manage PII securely. Posey [28] worked on categorizing the organizational PII breaching from text-mining and cluster analysis. This study founds 8 major PII-leaking types. On contrary, Non-Personally Identifiable Information (NPII) are shareable and risk free form of PII.

The first venture on Blockchain was the white paper of Bitcoin by Satoshi Nakamoto [29] presenting a fast cheap and transparent peer-to-peer transaction. Few jargons used frequently in Blockchain technology are as below:

Node: Node is a computer owned by any participating organization or user. Main activity of a node is to verify the transaction with other nodes before a block is added.

Consensus algorithm: A consensus is an algorithm used to approve any set of decision needed by the nodes.

Block: After a successful consensus, a new node with transaction or decision is added to current chain known as block.

Blockchain has used for identity management by several other studies. However, newly imposed EU-GDPR has bought a set of new regulations which will directly affect the way previous researchers were storing PII. Joshi [9] has combined data privacy and protection ontology and Blockchain technology. This study proposed a Linkshare system specially designed for big data where users can apply their customized regulations. Other studies have also used Blockchain technology for storing PII [10-11]. Benhamouda [10] used multiparty computation (MPC) and hyper ledger to store sensitive information. They implemented ‘chaincode’ to store and manage PII. Zyskind [12] created a platform that provides personalized user centric services by combining Blockchain as an access control consensus mechanism. Chen [13] described a framework which is based on cloud privacy managed by Blockchain. It suggests traceability of data and access to healthcare resources after an approval procedure.

The General Data Protection Regulation (GDPR) [14] came into effect from 25th of May, 2018 as a new privacy regulation for European Union (EU). This will also include any businesses, organizations and individuals outside of the EU have to comply with the Regulation if they are handling any sort of EU resident’s data [30]. A recent survey from around 2,000 IT professionals within the United Kingdom reported that only 47% of the respondents were fully aware of the GDPR while 41% reported they were aware but require more understanding on the subject and the last 9% they were not aware of it at all [30]. The GDPR [14], [30-32] have classified data handling organizations as controller and processor, defined as below.

Controller: Controller is those legal person or public authority who process PII of citizens from EU or member states.

Processor: Processer is those legal person or public authority who process PII information on behalf of controller.

III. PROPOSED METHOD

In this section, we advocate our proposed methodology for private Blockchain based Personally Identifiable Information (PII) Management System (BcPIIMS). First, we discuss architectural overview of our proposed method

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on April 16,2022 at 19:26:38 UTC from IEEE Xplore. Restrictions apply.

followed by functional properties. Final part provides detail use case scenarios for further elaboration.

A. Propsed Architecture:

Figure below (Fig.1) represent the overall architecture of our proposed system. Proposed system mainly deals with already defined three parties of GDPR they are: user, controller and processor. Proposed system provide a secure, transparent and GDPR friendly PII management system. Node and consensus algorithm are described below:

Node: User, controller and processor are three node type used in this study. Usually, PII data flows among these parties. In addition, Blockchain nodes are assumed to be located within the legal boundaries of GDPR.

Consensus Algorithm: This study uses a round robin (consensus algorithm) scheduling system, in which the permitted nodes (users, controllers and processors) must create blocks in rotation in order to generate a valid Blockchain. For robustness of the system, our mining diversity is set to 0.75 out of 0 to 1. That means for approving a new block to Blockchain at least 75 % of the total nodes must agree or response. This will save the system from freezing up if any set of miners become inactive for prolonged period. The overall working procedure is described below:

Firstly, users produced enormous amount of PII and NPII everyday while using several services offered by multiple organizations. Habitually, an organization collects PII either for providing a service or market analysis and prediction. Proposed system first delivers a list of PII, ρ or NPII, σ from a user, μ to controllers, $\alpha_{1\text{-}n}$. During this flow of information from μ to any α, a smart contract is signed between $\alpha_{1\text{-}n}$ to μ. Since, we already mentioned that GDPR does not allow preserving ρ on Blockchain, β. Therefore, proposed system is designed in a way that β stores only the σ achieved from μ. On the other hand, smart contract, η and NPII, σ and all other information except PII are stored in local database, Ω of each node (μ and α). Terms and conditions between two parties (μ and α) are signed as a smart contract, η. Where data privacy regulation, data using practice, data distribution procedures, notification process and mining techniques etc. are mentioned in detail. In another way, consensus between nodes (μ and α), will ensure the creation of a new smart contract, η which is then added as a new block to β (except PII). Hash of the local database, € is also added to that new block of Blockchain as a record of data flow.

In short, PII of the users are stored in off-chain local database of controllers. Similarly, Blockchain stores rest of the information with hash of that PII stored in local database. For any change of local database in controller side, user can easily identify that. Likewise, it would be easy to identify the set of responsible controllers in case of any PII breaching. Therefore, when a list PII passes from any user to a controller data stores as below:

Local data base, Ω = {ρ}
Blockchain, β = {η, σ, €, μ, α}

Secondly, controllers use several other processors for in detail analysis, market prediction, profiling, business model creation, consumer estimation etc. Therefore, a controller, α has to provides processor, $€_{1\text{-}n}$ a list of PII, ρ of user, μ. In this time all nodes (μ, α and €) undergoes for consensus. Like previous procedure, Blockchain stores all the Non-PII information and hash of PII. Oppositely, local database of each node (μ, α and €) stores users PII and send the hash of that PII into Blockchain. In other words, when all parties agreed upon the conditions of data sharing, a new block is added to existing Blockchain with hash of shared PII and NPII. Therefore, when a list PII passes from any controller to processor's data stores as below:

Local data base, Ω = {ρ}
Blockchain, β = {η, σ, €, μ, α, €}

As shown in fig. 1, upon successful consensus between user and controllers a new block is being added. Similarly, in case of processor, a block is added only after successful consensus from user, controller and related processor.

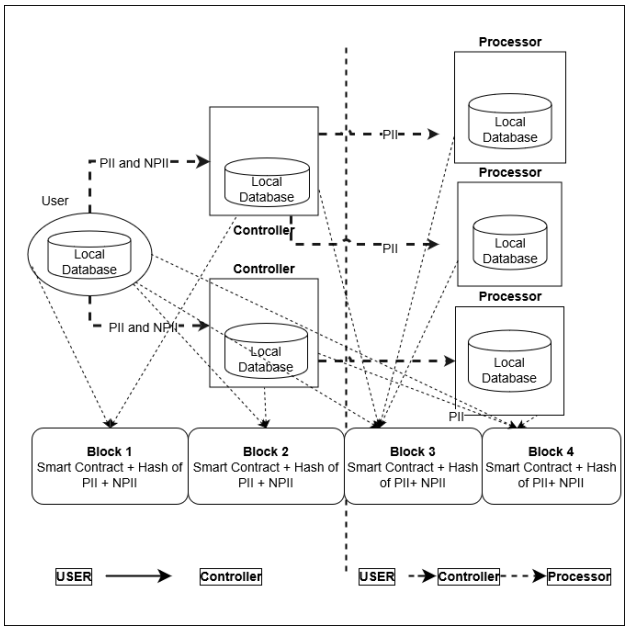

Fig. 1. Overall Architecture of the Proposed System

B. PII from User to Controllers:

1. Processing Personal data:

The user will share his Personal data with the controllers. The controllers will separate those data into Personally Identifiable Information (PII) and Non-Personally Identifiable Information (NPII) in order to do a separate storing mechanism. Afterwards, controller stores the PII in local database shown in Fig. 1 controller then generates a hash value of the shared PII and stores in Blockchain after consensus. After that a list of the data (PII, NPII) along with the hash value, terms and conditions will be published among nodes.

2. Consent and Smart Contract:

The terms and conditions for using the Personal Information of user along with the user consent will be created in a smart contract, and these terms and condition should also comply GDPR or similar data sharing rules and regulations.

3. Adding new Block to Blockchain:

The third step will be creating a Block containing the Smart contract, NPII and a Hashed value of PII, and adding the new Block into the Blockchain.

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on April 16,2022 at 19:26:38 UTC from IEEE Xplore. Restrictions apply.

C. PII from Controller to Processors:

1. Sharing Personal data:

The controllers shares the User personal data with the connected processors and informs the User with these updates and their purpose of sharing data to controllers. Processor again device PII and NPII data to stores separately. Then these data will be published between all nodes.

2. Consent and Smart Contract:

All nodes need to create a new smart contract holding terms and condition and the user's consent for using his Personal Information. After processor agreed upon all conditions given by controller and user, processer is now allowed to process those PII for data analyzing.

3. Creating a new Block:

After all the above the final step will be creating a new Block. This new block holds all smart contract, NPII and a hashed value of PII. A new block is then added to the existing Blockchain.

D. Sharing User's Personal Information's Scenarios:

Below a use case scenario is described in detail to elaborate the study in detail. Three scenario is added below they are: user-controller scenario, user-controller-processor scenario, delete and modify scenario.

1. User-Controller Scenario:

At the beginning (01) the User provides information to the controller (02) then the controller separates the data into PII and NPII and generate a hash value of the shared PII. (03) After separation of the data, a list of the data (PII, NPII) along with the hash value will be published between nodes. (04) Then a consensus of terms, conditions and the user's consent will be reached between the users. The controllers and this consensus needs to be compatible with GDPR regulation in order to be as a smart contract. (05) The final steps will be creating a Block holding all this information (Smart contract, NPII and a Hashed value of PII) and add as a new block to current Blockchain. As it is shown below in Fig. 2 for adding a new block 1 a consensus from both user and controller is taken into consideration.

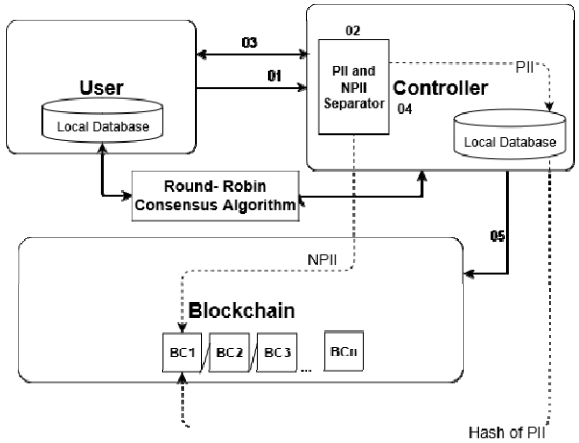

Fig. 2. User and Controller scenario

2. User –Controller-Processor Scenario:

After that, if a controller wants to share PII to processor for user data analysis (06). After separation of the PII and NPII processor informs the user and all three (user, controller and processor) reach in a consensus. And then a list of the data (PII, NPII) along with the hash value will be published between nodes. (07) This consensus is transformed into a smart contract and store into the Blockchain as a new. As it is shown below in Fig. 3 for adding Block number 2 a consensus from all parties are taken into consideration.

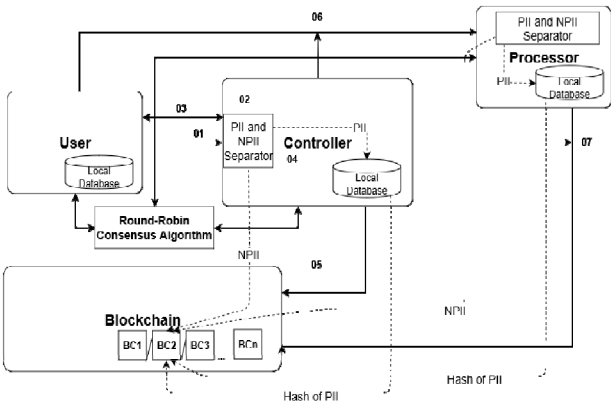

Fig. 3. User, Controller and Processor scenario

3. Delete and Modify Scenario:

The user informs all nodes of the need to delete/Modify his personal data from their Database. All nodes will then check the smart contract for the consensus between them and the user, which is stored in Blockchain. Afterwards, each of them does the deletion/modification on the user's data. Then a list of the deleted/modified data (PII, NPII) along with the hash value will be published between nodes. As it is shown below in Fig. 4 that as the hash from Blockchain is immutable so it remains same but actual data is no more. Finally, this hash is of no use without the actual data. This is how proposed system match as the GDPR regulation of data deletion. For the case of modify, as describes in fig. 5 after modification is done in local database hash is update to Blockchain as a new block. User can cross check the update by comparing the hash of the Blockchain data and hash of PII storing local database.

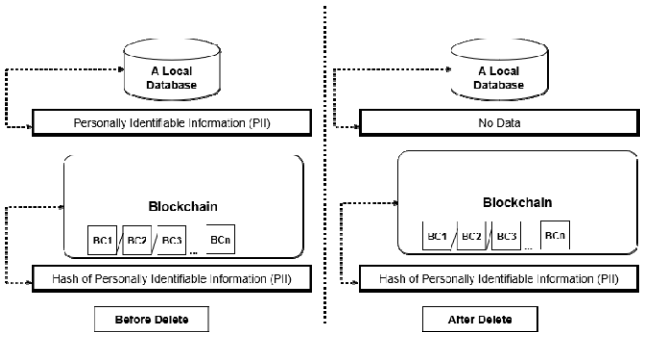

Fig. 4. Delete PII Scenario

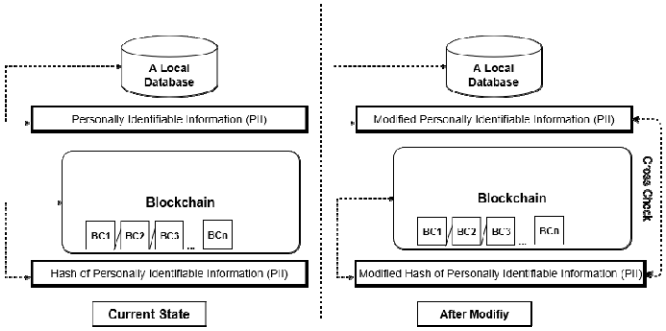

Fig. 5. Modify PII Scenario

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on April 16,2022 at 19:26:38 UTC from IEEE Xplore. Restrictions apply.

IV. Implementation and Discusion

This section presents the implementation of our proposed system and discuses some of the advantages it has comparing with the existing PII management and protecting systems.

1. System Implementation:

We have implemented a prototype of our proposed system on ten computers (Windows 10, i7-7700HQ CPU @ 2.8GHZ Samsung Inc. Republic of Korea) each representing a different participating entity such as user, controller, and processor. We implement it using the help of Multichain 2.0 an open source Blockchain implementation platform [33-34]. Our proposed method architecture is a private Blockchain, where the network consensus requires minimum difficulties to be achieved and maintaining the trust of third along participants (Round Robin). Nodes could also be defined or limited. Nevertheless, mining diversity is set to 0.75, flowing the Multichain implementation guideline. An example of our proposed system data storing (inside Blockchain data vs actual contract) is shown in the following Fig. 6.

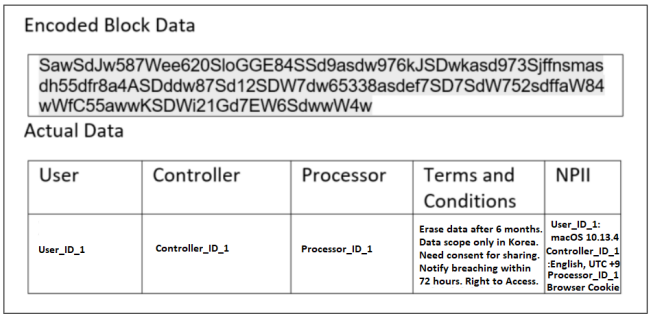

Fig. 6. Blockchain data Versus Actual data

2. Discussion:

We will now discuss few architectural difference and consequent advantages achieved by this study as below:

a) Storage:

Proposed method provides user with a copy of his own data directly from the controller, and also, a hash value of his own data, so the users are able to check and compare two hash values (i.e. one user has with the one stored in the Blockchain). Finally, this procedures ensure data authenticity.

b) Delete and Modify:

The user has the right to delete his personal data from both controller and processor, at any given time he wants. GDPR allows "The right to erasure" that means, new regulations allow user to modify or erase PII. To comply GDPR proposed BcPIIMS architecture also allow its user to modify and delete. A simple scenario is shown with Fig. 5 and Fig. 6. Since, off chain data is erasable and on chain storing of hash of PII and NPII is allowed that is how proposed system fully comply GDPR.

c) Security:

The consensus between the user, controller and processor will be stored securely in the Blockchain, so this consensus cannot be changed or altered. Therefore, the user can rest assured that the consensus is safe and can't be modified by adding or removing certain rules later. Blockchain "Data immutability". If any controller wants to distribute a new consensus will be needed from all parties. Since users are well aware of data storing the controller and processor, user can easily identify the defaulter which surely increases overall security of the PII.

d) Transparency and verification:

Proposed system can assure user that everything related to his data is transparent, the reason for using his data, to what purpose it is required and to whom his personal data is being shared with, all this information must be known to the user from the beginning till end. Also, the rules of the consensus must be intelligible, easily accessible and supported by all parties.

Now we present few core contributions of this study. As an ongoing work we hereby discuss the technical advantages:

First of all, after sharing of information from user to controller or even to processor proposed prototype can successfully track all kind of data manipulation. Since the suggested architecture keeps hash of all the PII data in an immutable Blockchain after consensus from all parties. If any controller or processor modify user PII then user can easily acknowledge that changes to take necessary action.

Secondly, user can easily predict the controllers or Processer by whom data has breaches. User can now which of his PII has shares with whom. Eventually, user can charge those controllers and processors for PII violation. Below we describe few more advantages of our proposed Blockchain based Personally Identifiable Information (PII) Management System (BcPIIMS).

Finally, proposed system offers additional data tracking and security enhancement just for using the blockchain technology along with a partially off-chain data storing mechanism. Normal data storing mechanism techniques considers both data and associated conditions as same priority. However, network attack, data purpose, privacy issues are classified into several ranges [35]. Proposed off-chain blockchain emphasize the regulations or data handling rules to store in on chain. Although, PII information are stored in off-chain but their hash are stored on-chain along global approval procedure makes the tampering difficult. Above causes justify the using of off-chain data storing and blockchain together which are totally absent in typical practices.

Future goal of this study is to present an in detail numerical comparison with exiting system. Since, the work is on progress, we present the technical advantages of this work theoretically. Similarly, IoT equipment generated personal data management system will be developed as a real life implementation of this study. Similarly, developing a GDPR complied big data management technique assisted by gradual learning from system is our future objective.

V. Conclusion

In this paper, to reduce the risk of Personally Identifiable Information (PII) leaking we propose a system called Blockchain based Personally Identifiable Information (PII) Management System (BcPIIMS). Our proposed models are capable of tracking the life cycle of PII throughout the controllers and processors. By storing the data in off-chain the system will be complying with GDPR rule (Right to be forgotten) since the off-chain data can be deleted at any time where only the hash of the data remaining in the Blockchain is of no use. Our research reveals that the proposed model ensures higher security and comply privacy regulations.

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on April 16,2022 at 19:26:38 UTC from IEEE Xplore. Restrictions apply.

Furthermore, misuse, mismanagement and lesser scope for PII tracking were identified by several studies. Using off chain Blockchain and data hash checking our proposed system successfully addressed those problem. Therefore, proposed system will have significant effect to secure PII. Future research direction is to develop a fully-fledged PII tracking and managing system for a secure PII flow.

ACKNOWLEDGEMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (Ministry of Science and ICT) (No.2018-0-00261, GDPR Compliant Personally Identifiable Information Management Technology for IoT Environment)

REFERENCES

[1] Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17.

[2] Solutions, V. E. (2015). Data Breach Investigations Report. Verizon, Report.

[3] Kobezak, Philip, Randy Marchany, David Raymond, and Joseph Tront. "Host Inventory Controls and Systems Survey: Evaluating the CIS Critical Security Control One in Higher Education Networks." In Proceedings of the 51st Hawaii International Conference on System Sciences. 2018.

[4] Armerding, T. (2018, January 26). The 17 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[5] First Half 2017 Breach Level Index Report: Identity Theft and Poor Internal Security Practices Take a Toll. (n.d.). Retrieved May 19, 2018, from https://www.gemalto.com/press/pages/first-half-2017-breach-level-index-report-identity-theft-and-poor-internal-security-practices-take-a-toll.aspx

[6] Sands, M. (2018, January 17). Why Customer Data Is Trade Marketing's New Currency. Retrieved from https://www.forbes.com/sites/mikesands1/2018/01/17/why-customer-data-is-trade-marketings-new-currency/#2d5a2f33d199

[7] Miraz, M. H., & Ali, M. (2018). Applications of Blockchain Technology beyond Cryptocurrency. arXiv preprint arXiv:1801.03528.

[8] Onik, Md Mehedi Hassan, Miraz, M. H, and Chul-Soo Kim. (2018) "A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0" in Proceeding Smart cities Symposium 2018, Bahrain (pp. 11-16). IET

[9] Joshi, K. P., Gupta, A., Mittal, S., Pearce, C., Joshi, A., & Finin, T. (2016, December). Semantic approach to automating management of big data privacy policies. In Big Data (Big Data), 2016 IEEE International Conference on (pp. 482-491). IEEE.

[10] Benhamouda, F., Halevi, S., & Halevi, T. (2018, April). Supporting private data on Hyperledger Fabric with secure multiparty computation. In Cloud Engineering (IC2E), 2018 IEEE International Conference on (pp. 357-363). IEEE.

[11] Bahri, L., Carminati, B., & Ferrari, E. (2018). Decentralized privacy preserving services for Online Social Networks. Online Social Networks and Media, 6, 18-25.

[12] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using Blockchain to protect personal data." Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015.

[13] Chen, L., and Hoang, D.B.: Novel data protection model in helthcare cloud. In: 2011 IEEE 13th International Conference on High Performance Computing and Communications (HPCC), pp. 550-555. http://dx.doi.org/10.1109/HPCC.2011.48

[14] Regulation (EU) 2016/679 (General Data Protection Regulation) https://gdpr-info.eu/art-4-gdpr/

[15] Rt.com. Obama announces legislation protecting personal data, student digital privacy, 2015.

[16] Borgman, C. L., & Kay, D. G. (2017). Faculty Engagement to Reduce PII (Personally Identifiable Information) Risk.

[17] Weingärtner, R., & Westphall, C. M. (2017, August). A design towards personally identifiable information control and awareness in OpenID Connect identity providers. In Computer and Information Technology (CIT), 2017 IEEE International Conference on (pp. 37-46). IEEE.

[18] J. Brill, FTC (2012). Big Data Issues. Retrieved from https://www.ftc.gov/publicstatements/2012/03/bigdata-big-issues

[19] Alduaij, S. (2017). Data Mining Approach to Compare Privacy Policies. University of Maryland, Baltimore County.

[20] Legislative Services Branch. (2018, May 04). Consolidated federal laws of canada, Personal Information Protection and Electronic Documents Act. Retrieved May 19, 2018, from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

[21] Department. (2018, April 06). Notifiable Data Breaches scheme - Office of the Australian Information Commissioner (OAIC). Retrieved May 19, 2018, from https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

[22] ISO/IEC 27000 family - Information security management systems. (2017, August 29). Retrieved May 19, 2018, from https://www.iso.org/isoiec-27001-information-security.html

[23] Pfitzmann, A., & Hansen, M. (2005). Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology.

[24] McCallister, E., Grance, T., & Scarfone, K. A. (2010). Guide to protecting the confidentiality of personally identifiable information (PII) (No. Special Publication (NIST SP)-800-122).

[25] Juan Perez. Facebook, google launch data portability programs to all, 2008.

[26] McCallister, Erika. Guide to protecting the confidentiality of personally identifiable information. Diane Publishing, 2010.

[27] McCallister, Erika, Timothy Grance, and Karen A. Scarfone. Guide to protecting the confidentiality of personally identifiable information (PII). No. Special Publication (NIST SP)-800-122. 2010.

[28] Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, *26*(6), 585-604.

[29] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[30] MARTIN, DR GEORGIA, and SERGE PALLADINO. "What is GDPR, Why it is Needed & How to Prepare." (2017).

[31] General Data Protection Regulation (GDPR) – Final text neatly arranged. (n.d.). Retrieved from https://gdpr-info.eu/

[32] Voss, W. Gregory. "European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting." (2017).

[33] Multichain white paper (2015) Available: https://www.multichain.com/download/Multichain-White-paper.pdf

[34] Greenspan, G. (2018, January 29). Second MultiChain 2.0 preview release. Retrieved February 1, 2018, from https://www.multichain.com/blog/2018/01/secondmultichain-2-0-preview-release/

[35] Onik, M. M. H., Al-Zaben, N., Hoo, H. P., & Kim, C. S. (2018). A Novel Approach for Network Attack Classification Based on Sequential Questions. *arXiv preprint arXiv:1804.00263*.

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on April 16,2022 at 19:26:38 UTC from IEEE Xplore. Restrictions apply.