

A Conceptual Framework for Securing Privacy and Optimization of Personally Identifiable Information

Raghavendra T.S¹

Research Scholar, VTU, Belgaum
raghavendra.srirama@gmail.com

Dr. K.G. Mohan²

Professor, Dept. of CSE, SVIT, Bangalore
mohankabadi62@gmail.com

Abstract— In the period of pervasive distributed computing condition each individual likes to complete work on the web however it forces most noteworthy danger of divulgence of one's Intellectual data, for example, by and by identifiable information(PII), which can be identified with keeping money, training, medicinal services et cetera. With a specific end goal to confront any such helpless assaults in the cloud by and by part of research work is going on. In this paper we show a significant calculated stringent structure which takes after a proactive way to deal with handle any kind of information breaks assaults.

Keywords: Personally-identifiable information(PII) , Data Breach, Framework

I. INTRODUCTION

THIS Identity burglary has been a biggest risk for human humankind and now which has turned into a viral wherever in the globe. It circularly expanding on the web each day and has influenced around seventeen and half million people in 2014 [1]. Data fraud is a major wrongdoing which forces significantly three risks that hide on the web, which are digital tricks, stalkers and taking where the misleading procurement and utilization of a man's Personally Identifiable Information (PII) is occurring. The data is being partaken in different routes some of them are interpersonal organizations, instructive, medicinal services data and alongside other IoT area exercises. These days association on informal organizations has outflanked all other online exercises, which can be considered as a one of the best web action. With raised online investment and information sharing brings the danger of achieving data to numerous foes. Which has obviously defended a need to ensure our PII on the web. To help obtaining of online protection, Privacy as an administration [2], [3], [4] is drawing in consideration of numerous scientists and businessman's. [6] proposes a strategy to manage customer side recognition and investigation of PII taking trackers which are sent by outsider sites to exploit by taking customer's impression and later utilizing it for business purposes, for e.g., directed advertising.

Keeping in mind the end goal to avoid personality hoodlums and fraudsters, a first activity is understanding what constitutes a man's character in both the digital and physical universes. By and by the virtual digital movement has turned into another piece of our regular day to day existence, which attracts a man's PII to wind up noticeably a consistently complex mixing of their life. Cases for on-line traits are one's scholarly data such online networking accounts, medicinal services data relating to their present and past medical problems, one's instructive data, on-line e-keeping money, shopping examples and email accounts. Disconnected properties incorporate those which speaks to one's physical biometric information, for example, unique mark designs [5].

The rest of this paper is organized as follows. Section II presents related work about frameworks to manage PII along with optimization techniques. Section III present work done w.r.t healthcare, education, social networks, Section IV describes the different methods used for anonymization of PII, Section V presents discussion and summary.

II. RELATED WORK

In [7] Web of Objects(WoO) based pervasive administrations and system for safeguarding the protection have been proposed to deal with and secure the security of Personal Identifiable Information (PII). The WoO empowers every single physical protest, correspondence and web availability to bring out and devour the data. [7] likewise proposes a versatile, handy and bargaining security structure engineering of WoO based pervasive administrations to deal with the arrival of client PII to some other clients and outsider serving providers. They additionally recommend PII framework for powerfully adjust to any client PII, protection settings framework for adoptability and bargaining of client security settings control, and XACML which is an adaptable markup dialect for Accessing Control and permitting the interoperability among various merchants. The proposed design depends on REST for lightweight and superior like deft based one. They at long last present the administration situations of client PII gathering, and presenting the data to others clients like outsider specialist organizations. At the point when protection of PII is viewed as then its meta-structure information likewise ought to be considered in that viewpoint [8] presents an applied system with the point of furnishing the security alongside the protection for vital data.

Giving protection and securing PII should be a continuum factor, in the event that it incorporates information minimization of PII then it can significantly be valued. In [9] an applied structure of big business security engineering has been proposed keeping protection continuum and information minimization of PII as the key elements. Which mostly looks at one's close to home data put stock in support of handle more quick witted city data and offers information securely crosswise over various different offices inside a city. The proposed brilliant security stage is an open and close administration stage which can without much of a stretch be implanted into each savvy framework. Its venture security engineering is a protection administration show which has four layered administrations measurement in accumulation and care of PII. PII in the keen frameworks can unintentionally recognize a person with joining distinguished and identifiable PII. They at last proposed an answer for diminish dangers of unintentionally distinguishing a person in social administrations of a shrewd city.

To protect security of PII while sharing on the web, strategies of anonymization and cleansing are especially vital. In [10] an Iterative Classification technique for the Sanitization of Large-Scale Datasets has been proposed. Their voracious calculation permits sharing of more than 93% unique data. Their proposed technique for cleaning extensive scale information is an exertion which is expected to deal with a lot of unstructured data that is gathered over various spaces which is restricted by the touchy information contained in it. [11] proposes k-anonymization specialized approach which chips away at settled esteemed system hub data. Their proposed calculation accomplishes k-secrecy by limiting the expansion and cancellations operations. Their examinations result on genuine numerical dataset demonstrates that, less number of operations are adequate than other concealment based methodologies. [12] additionally proposes a Privacy shield as a system for Preserving Privacy for people alongside

the assurance of PII. They make utilization of open key framework alongside their use of data System Hippocratic Policies for accomplishing information secrecy, with the goal that data arrangement of client's close to home information is saved.

Giving security to PII over cloud isn't a simple undertaking, primarily it is important part for spaces like Healthcare, instruction, online networking and back. In that point of view loss of data can occur in a few routes few of them in like manner are, 1) web based business exchanges incorporate electronic exchanges by means of online installment application, 2) nearness of numerous specialized controls rules, 3.) absence of oversight for PII assurance while perusing. 4) permitting remote-get to answers for outsiders can bring about risk. 5) Multiple trusted systems a trade off at one site can endanger a few different properties.

III. REQUIREMENTS AND PRIVACY CHALLENGES IN EDUCATION, HEALTHCARE, SOCIAL MEDIA AND IoT

A. Privacy in Education

An open cloud stage offers funds, simplicity of administration, and flexibility to arrangements. What's more, regulative compliancy and assurance must be guaranteed for arrangements dealing with touchy data, for example, understudy and medicinal services information. With the over the top ascent in data breaks everywhere undertakings, it is a need to give significance for the security, protection, and consistence of cloud-controlled arrangements that hold PII. A case of an answer needing such confidences is an instruction and learning-related examination benefit that oversees classified understudy information on an open cloud stage. [13] have proposed an approach for dealing with the security and protection of a training and learning-examination arrangement on an open cloud stage while promising similarity with the Family Educational Rights and Privacy Act (FERPA). [13] Additionally propose another deft organization system which is both rapid and automated. A model of a learning-examination arrangement was executed on a Soft Layer open cloud, and the new sending procedure was assessed in correlation with existing techniques.

B. Privacy in healthcare

A wellbeing interpersonal organization is one of the online information benefit which encourages data preparing among nearly connected individuals from a group with the same or a comparable wellbeing thought. Over the past numerous years, numerous mechanical recommender frameworks have been produced for long range informal communication keeping in mind the end goal to enable clients to discover their groups of intrigue. [14] presents a perfect wellbeing long range informal communication as a model for estimating the likenesses of patients. And, after its all said and done likewise it isn't significant to share any such delicate and private information over the Internet. [14] has new information offering plan to that every last patient is considered as d-words (discriminant words) and those d-words are utilized to assess characters between patients without unveiling their identifiable individual information. The d-words are straightforward in nature like "shop," and consequently don't contain delicate individual information. that makes their strategy as a proficient one. Presently with their plan sharing of d-words on the Internet is anything but difficult to discover matches who may have comparable wellbeing contemplations [14].

In [15] a sensible business insight apparatus based social insurance system has been exhibited. It makes utilization of measurable and information mining procedures as center systems in building up the model. [15] gives information covering strategies to limit and to safeguard the PII. [15] propose a useful arrangement segment for an implicit

information covering system. It distinguishes delicate data and chooses best covering group with a specific end goal to give more information security and assurance. [16] discusses issues of protection and exposure of clinical genomic examine data and important rules which saves one's security while sharing the hereditary data to others for investigate reason. [17] talks about a technique for disinfection to the person's close to home wellbeing records, for example, pathology records, in this they take after semantical way to deal with secure delicate data. [18] proposes answer for share PII by utilizing a calculation that utilizes l-decent variety alongside the pseudonymisation procedure to keep the harmony between data handling and its use in healing centers, research and open purposes.

C. Privacy in Social media

In display days' parcel of individuals are partaking in online interpersonal interaction locales, as "Facebook, Twitter". Considering the protection perils of unveiling PII, a ton look into has been done to abstain from falling data to wrong hands. Directly numerous controls like gatherings, records alongside circles have been acquainted with handle security.

[19] propose a model for assessing protection scores of companions from singular foe clients' point of view. From the assessed comes about one's information sharing conduct and who sees what data can without much of a stretch be found. Assessment of Privacy Scores are finished utilizing protection scoring utilitarian element with the assistance of cubic Bezier bend [19]. [20] considers a profiling and following assault which corresponds a guest's online conduct that is caught from an obviously pure site with that of a similar guest's genuine Facebook profile. An examination is made with caught investigation and from an adaptable Facebook Fan Page to guarantee that how they can recognize the guest when just their online persona is given. They break down online part of 25 members with around 64% of accuracy lastly gives protection instruments to the online clients [20]. In [21] trial comes about say that understudies are have a tendency to unveil PII on theirs profiles and in this manner they can be considered as daring people and it is all from south African understudies' specific situation yet not in nonexclusive setting.

Clients' readiness to take an interest in sharing PII by means of person to person communication administrations is affected by a few variables. [22] presents an arrangement of developmental constituents which can structure the individual esteem framework and their causal strategy clarifies the connections among the proposed builds. Proposed static Trust factors are inclination, past-conduct and socioeconomics and verbose trust factors are enthusiastic state, saw estimation of results, intermediary trust, nature and need [22]. Aside from customary system assaults, malevolent crawlers focus on person to person communication destinations is a biggest danger to the digitalized information. [23] presents a connection encryption model to check with pernicious crawlers and their tests on the created model shows agreeable outcomes to adequately protect any noxious crawler's assaults.

Each Web client associates with a specialist co-op by means of a Web program utilizing a solitary sign-on WebID, tending to the examination difficulties of protection saving WebID investigation isn't a straightforward errand, a protection mindful engineering has been introduced to veil PII and other delicate information. They prescribe use of RHadoop, for a compelling huge scale investigation of informal community connected datasets. Presents two kinds of WebID Analytics 1) Unifying Anonymized WebID for investigation and 2) R and Hadoop for

WebID examination alongside two arrangements for information dealing with they are Semantics-empowered approaches and access control strategy [24]. Playing diversion online gives others to take in more about the players, with that gathered information enemies a chance to can undoubtedly separate PII, which puts client at information spillage setting [25].

D. Privacy in IoT

Web of Things (IoT) covers the balanced association of unmistakable gadgets which are competent with promissory administrations through their participation. The participation between gadgets in such an IoT cloud condition regularly requests for bona fide and wanted individuals to give helpful administrations to the end client. Appropriately, before conceding them as individuals from an IoT situation needs to evaluate the trustworthiness levels of each one of those gadgets. Display trust assessment models make utilization of assets, for example, recorded perceptions or proposals information to evaluate the put stock in level of a gadget. Be that as it may, these present assessment frameworks come up short on the off chance that it doesn't locate any current put stock in asset. [26] presents a perfect IoT framework called individual space IoT and recommends another trust assessment display which executes a test reaction trust evaluation to gauge the credibility level of a gadget before conceding it to partake in the space. Their trust evaluation show does not take after the present customary strategies. The proposed challenge-reaction credibility assessment display measures the vulnerability about the gadget's conduct by means of entropy and afterward makes an interpretation of the related entropy to trust esteem [26].

On the planet Internet of Wearable things(IoWT), data assembled at their capacity framework is tremendous. In such gigantic measure of gathered information, taking care of PII is especially chance factor. [27] presents a novel secure strategy to help the impermanent sharing of wearable things with others. Phishing is the primary issue experienced alongside different issues like protection, Relay assaults, Downgrade, Malicious wearable, wearable gadget trading off and arrange flow dangers with the wearable-particular gadget assignment convention [27]. To address the security factor [28] proposes an utmost for the utilization of sensors to just Bluetooth, RFID and those sensors which catch alphanumeric information. To such an extent that human exercises are unequivocally spoken to alongside gadgets ID's, which can limit the PII gathered. Since less data is gathered it winds up plainly troublesome for assailants to recognize clients' data. [29] handles User-Generated administrations (UGS) by giving different security and data insurance concerns.

[30] Introduces a protection mindful framework which gathers client data in light of their impressions. Considering impression following framework rather than picture acknowledgment lessens part of uneasiness. the outcomes demonstrate that it can without much of a stretch recognize clients by 94%. [31] proposes an application to deal with security of transportation frameworks, for example, autos. Their proposed CANE framework does every one of the assignments to diminish the danger of potential security spills in dispersed Intelligent Transportation Systems. Which improves client ability to oversee security properties while in the meantime supporting application prerequisites.

IV. VARIOUS TECHNIQUES TO HANDLE ONLINE WEB INFORMATION PRIVACY

[35] proposes a grouping calculation as a way to deal with enhance the assorted variety of anonymized information. Proposed calculation evaluated with grouped type of a unique genuine dataset. The results are assessed as for its ease of use in logical works and it was watched that both bunching and

anonymization calculations ought to be utilized to keep assorted variety of this present reality unique datasets. [36] presents a Privacy Impact Assessment(PIA) format for taking care of dangers which emerges from provenance diagrams (implies a chart with joins educating who and which exercises are made, utilized and changed elements) in an application-freethinker setting. Distinguishing security dangers and setting up countermeasures is of central significance when provenance is conceived in open frameworks, for example, the web [36].

Security of the outsourced data is one of the more noteworthy test. [37] proposes a component to store private information and secure recovery of this data utilizing an emit sharing framework based secure multi-party Computation(SMC). Their fundamental thought is to actualize a system to store such private information with an exceedingly accessible capacity supplier which is available from anyplace with the assistance of questions while subtly concealing the first data esteems from the capacity supplier [37]. With the expanded movement in open disseminated situations such e-exchanges, web based business, giving security to such shared data is particularly basic issue. [38] presents a model where individuals have the alternative to quit from letting the individual data to be caught for a result esteem which can balances the expenses of protection. Their model is made for the benefit of considering working operators with the enthusiasm of buyers to increase their pick up. The outcomes demonstrate that clients and specialist co-ops are both happier if security chance is low.

[34] presents a joined expert rules and models with strategies to deal with the security concern. They first shows utilization of a three-layered model for client protection worries as for framework operations, for example, data stockpiling, exchange and preparing and assess their outcomes on client conduct. Next they create rules for building security ideal frameworks. They recognize and propose two methodologies for designing protection: initial one "security by-arrangement" and second one "security by-engineering". The main approach concentrates on the advancement of the notice and decision standards of reasonable information rehearses, while other approach cuts down the accumulation of PII and anonymization with customer side data stockpiling and preparing [34].

Perception of information is basically done to effortlessly comprehend and examine any given plotable information gave it keeps up the required info information structure. Before making utilization of any information, de-distinguishing proof process is done to save the PII. Notwithstanding, the past examination says that, as a few datasets are uncovered on open, the more noteworthy possibility of abusing the information by joining a few related information table with comparative highlights. This kind of protection re-recognizable proof is by and large excessively confounded or indistinct, making it impossible to be acknowledged by data proprietor. In January 2013, numerous South African organizations were hacked, which brought about the security break with 700000 records. The intension of [33] is to inspect and investigate profoundly the data delivered from the South African information infringement and to envision the effect on the organizations. The information which was separated for investigation reason for existing is basically PII, which is alluded by the

Electronic Communications and Transactions Act of 2002 and the Protection of Personal Information Bill of 2009 [33]. [32] proposes a novel open information de-distinguishing proof perception examination device (ODD Visualizer) to affirm whether there exists delicate information spillage issue in the objective datasets or not. The high adequacy, that ODD Visualizer can render, chiefly comes through actualizing adaptable processing stage alongside creating viable

information representation method. [32] Demonstrates and demonstrates that ODD Visualizer to be sure revealed one genuine defenselessness of record linkage assault among open datasets accessible on the web.

V. DISCUSSION



Figure 1. conceptual framework for secure transfer of private information with optimization of PII.

In nowadays' information ruptures is a comprehensively developing issue. Security records are being stolen by the millions in online breaks [39] [44] and others individual touchy data is being utilized for monetary profit too [43]. There is a need of institutionalized model with numerous techniques for taking care of security dangers for every personality life cycle, for example, Identity arrangement, proliferation, utilization and upkeep, and annihilation, and the criteria which can survey the protection insurance level proposed by the Identity provider as a stage against these dangers [40] [41]. Keeping in mind the end goal to have such an institutionalization for ensuring the PII while sharing one's delicate data, existing strategies like information anonymization, de-recognizable proof with covering philosophies have been introduced to handle online protection factors. At the point when arrangement is considered at worldwide level we would confront the security hazard at enormous information level, in such cases, a large number of the significant models have been displayed, for example, Hadoop. In any case, all the displayed arrangements relating to the data protection are of relatively particular to their own particular issue explanations. Nonetheless, having a system with non specific institutionalized security arrangements would help the information breaks issues in worldwide satisfactory sense. The work did in this paper is one such errand to link best accessible procedures and after that to propose nonexclusive security approaches with a system which can deals with the PII everywhere scale with improvement methods.

VI. CONCLUSION

In this work a conceptual framework (Figure 1) has been presented in order to securely store, transfer and process data among multiple users. It mainly considers following factors. 1) TTP services for securely share the data with on-demand send and request policy. 2) Threat intelligence component architecture to securely anonymize the data. We believe that the proposed framework can successfully manage any threats from attackers with the proactive defense mechanisms.

APPENDIX

PII-Personally Identifiable Information

WoO- Web of Objects

XACML-Extended Access Control Markup Language

RAST-Representational State Transfer

ACKNOWLEDGMENT

My Sincere thanks to Mr. Lohith N, PG Student for helping in writing this paper.

REFERENCES

- [1] E. Harrell, Bureau of Justice Statistics, US Dept of Justice, and Office of Justice Programs, "Victims of identity theft, 2014," 2014.
- [2] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures". In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pages 711–716, 2009.
- [3] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the facebook platform". In Proceedings of Web, volume 2, 2009.
- [4] B. Vidyakshmi, R. K. Wong, M. Ghanavati, and C. H. Chi, "Privacy as a service in social network communications". In IEEE International Conference on Services Computing (SCC), pages 456–463, 2014.
- [5] Razieh Nokhbeh Zaeem, Suratna Budalakoti and K. Suzanne Barber, Muhibur Rasheed and Chandrajit Bajaj, "Predicting and Explaining Identity Risk, Exposure and Cost Using the Ecosystem of Identity Attributes". In Proceedings of IEEE 2016.
- [6] Shivani Thapar, Neetika Srivastava, Anup Girdhar, Aruna Bhat, "Host based Detection and Analysis of PII Stealing Trackers". International Conference on Computing, Communication and Automation (ICCCA) 2016.
- [7] Muhammad Ansar Latif, Farman Ullah, Sungchang Lee, "Extensible Privacy Framework for Web of Objects Based Ubiquitous Services", In Proceedings of IEEE 2015.
- [8] Geoff Skinner, Song Han, and Elizabeth Chang, "Defining and Protecting Meta Privacy: A New Conceptual Framework Within Information Privacy". Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW'06), 2006.
- [9] Yutaka Mizuno, Nobutaka Odake, "A Privacy continuum in a conceptual framework of enterprise privacy architecture", Proceedings of PICMET '16: Technology Management for Social Innovation 2016.
- [10] 'Bo Li, Yevgeniy Vorobeychik, and Muqun Li, Bradley Malin', "Iterative Classification for Sanitizing Large-Scale Datasets", IEEE International Conference on Data Mining 2015.
- [11] Shyue-Liang Wang1, Yu-Chuan Tsai, Hung-Yu Kao2, Tzung-Pei Hong, "Anonymizing Set-Valued Social Data". IEEE/ACM International Conference on Green Computing and Communications & IEEE/ACM International Conference on Cyber, Physical and Social Computing 2010.
- [12] 'Geoff Skinner, Song Han and Elizabeth Chang', "A Framework of Privacy Shield in Organizational Information Systems". Proceedings of the International Conference on Mobile Business (ICMB'05) 2015.
- [13] Yasuharu Katsuno, Ashish Kundu, Koushik K Das, Hitomi Takahashi, Robert Schloss, Prasenjit Dey and Mukesh Mohania "Security, Compliance, and Agile Deployment of Personally Identifiable Information solutions on public cloud". IEEE 9th International Conference on Cloud Computing 2016.
- [14] Insu Song and Nigel V. Marsh "Anonymous Indexing of Health Conditions for a Similarity Measure". IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 16, NO. 4, JULY 2012.
- [15] 'Osama Ali and Abdelkader Ouda', "A Classification Module in Data Masking Framework for Business Intelligence Platform in Healthcare". proceedings of IEEE 2016.
- [16] 'Dov Greenbaum, Arif Harman, Mark Gerstein', "Proposed Social and Technological Solutions to Issues of Data Privacy in Personal Genomics", proceedings of IEEE 2014.
- [17] 'Wei Jiang, Mummoothy Murugesan, Chris Clifton, Luo Si' "t-Plausibility: Semantic Preserving Text Sanitization". International Conference on Computational Science and Engineering 2009.
- [18] 'Rose Tinabo, Fred Mtenzi, Ciaran O'driscoll and Brendan O'Shea', "Solving the Problem of Balancing Data Usefulness and Protection of Personal Identifiable Information using Multiple Anonymisation Techniques". Proceedings of IEEE 2009.
- [19] 'Vidyakshmi B.S', 'Raymond K. Wong', 'Chi-Hung Chi', "Privacy scoring of social network users as a service". IEEE International Conference on Services Computing 2015.
- [20] 'Jason W. Clark', "Correlating a Persona to a Person". ASE/IEEE International Conference on Social Computing and ASE/IEEE International Conference on Privacy, Security, Risk and Trust 2012.
- [21] 'Sayed Enayat Sayed Ally, Craig Blewett and Brett van Niekerk', "Facebook: The Risk-Taking Attitude amongst Emerging Adults". Proceedings of the IEEE 2014.
- [22] 'Daniel Long', Simon Cleveland', "Toward a Privacy Model for Social Networking Services". Proceedings of the IEEE SoutheastCon 2015, April 9 – 12 - Fort Lauderdale, Florida 2015.
- [23] 'Sri Khetwat Saritha', 'Kishan Dharavath', "Link Encryption to Counteract with Rouge Social Network Crawlers". Ninth International Conference on Information Technology- New Generations 2012.

- [24] 'Yuh-Jong Hu', "Privacy-Preserving WebID Analytics on the Decentralized Policy-Aware Social Web", 2014.
- [25] 'Dragana Martinovic, Victor Ralevich, Joshua McDougall, and Michael Perklin', "You are what you play" Breaching privacy and identifying users in online gaming". IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT). Twelfth Annual Conference on Privacy, Security and Trust (PST) 2014.
- [26] Tham Nguyen, Doan Hoang, Aruna Seneviratne, "Challenge-Response Trust Assessment Model for Personal Space IoT". The First IEEE International Workshop on Security, Privacy and Trust for IoT, 2016.
- [27] 'Aleksandr Ometov, Sergey Bezzateev, Joonas Kannisto, Jarmo Harju, Sergey Andreev, Yevgeni Koucheryavyy' "Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things". IEEE Internet of Things Journal, 2016.
- [28] 'Dennis Lupiana, Fredrick Mtenzi, Ciaran O'Driscoll, Brendan O'Shea', "Strictly Alphanumeric Data: Improving Privacy in Smart Environments", 2011.
- [29] 'J. C. Yelmo, C. Martínez, J. M. del Álamo and M. A. Monjas', "Protection of Personal Information in User-centric Converged Service Platforms". IEEE LATIN AMERICA TRANSACTIONS, VOL. 8, NO. 2, APRIL 2010.
- [30] 'Ryoya Wada, Shigeaki Tagashira, Masaki Ogino, Shigemi Ishida, and Akira Fukuda', "A Privacy-aware User Tracking System Using Footprint Data Measured Across Multiple Pressure sensor sheets". 5th IIAI International Congress on Advanced Applied Informatics, 2016.
- [31] 'Stefan Dietzel, Martin Kost, Florian Schaub, and Frank Karg', "CANE: A Controlled Application Environment for Privacy Protection in ITS". 12th International Conference on ITS Telecommunications 2012.
- [32] 'Chiun-How Kao, Chih-Hung Hsieh, Yu-Feng Chu and Yu-Ting Kuang', "Using Data Visualization Technique to Detect Sensitive Information Re-Identification Problem of Real Open Data Set". International Computer Symposium, 2016.
- [33] 'I.P. Swart, M.M. Grobler, B. Irwin', "Visualization of A Data Leak". Proceedings of the IEEE 2013
- [34] 'Sarah Spiekermann and Lorrie Faith Cranor', "Engineering Privacy". IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 35, NO. 1, JANUARY/FEBRUARY 2009.
- [35] 'Pelin CANBAY', 'Hayri SEVER'. "The Effect of Clustering on Data Privacy". IEEE 14th International Conference on Machine Learning and Applications, 2015.
- [36] 'Jenni Reuben, Leonardo A. Martucci, Simone Fischer-Hubner', "Privacy Impact Assessment Template for Provenance". 11th International Conference on Availability, Reliability and Security, 2016.
- [37] 'Divya G Nair', 'Binu. V.P.', 'G. Santhosh Kumar', "An Effective Private Data storage and Retrieval System using Secret sharing scheme based on Secure Multi-Party Computation". International Conference on Data Science & Engineering (ICDSE), 2014.
- [38] 'Abdulsalam Yassine, Ali Asghar Nazari Shirehjini, Shervin Shirmohammadi, Thomas T. Tran', "Online Information Privacy: Agent-Mediated Payoff", Ninth Annual International Conference on Privacy, Security and Trust, 2011.
- [39] 'Danny Bradbury', "Fighting ID theft", 2016.
- [40] 'Hyangjin Lee, Inkyoung Jeun, Hyuncheol Jung', "Criteria for evaluating the privacy protection level of Identity Management services". Third International Conference on Emerging Security Information, Systems and Technologies, 2009.
- [41] 'Chien-Cheng Huang', 'Kwo-Jean Farn', 'Frank Yeong-Sung Lin', "A Study on Information Security Management with Personal Data Protection". IEEE 17th International Conference on Parallel and Distributed Systems, 2011.
- [42] 'Abdul Sattar Raja', 'Dr. Shukor Abd Razak', "Analysis of Security and Privacy in Public Cloud Environment". Proceedings of the IEEE 2015.
- [43] 'Il-Horn Hann', 'Kai-Lung Hui', 'Sang-Yong Tom Lee', 'Ivan P.L. Png', "Analyzing Online Information Privacy Concerns: An Information Processing Theory Approach". Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
- [44] 'Linda Wilbanks', "The Impact of Personally Identifiable Information", White Paper IT Pro July 1 August 2007.

