IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 24, No. 5, October, 2019, pp. 531-537
Journal homepage: http://iieta.org/journals/isi

A Secured Framework to Protect Association Rules in the Big Data Environment Using Fuzzy Logic

Sake Madhu[1], Ranjit Reddy Midde[2], Gandikota Ramu[3*], Appawala Jayanthi[3], Jalari Somasekar[4], Gajula Ramesh[5], Pallela Dileep Kumar Reddy[6]

[1] Dept of Computer Science & Engineering, Guru Nanak Institutions Technical Campus, Telangana 500043, India
[2] Dept. of Computer Science and Engineering, Srinivasa Ramanujan Institute of Technology, Anantaphuramu 515001, India
[3] Dept of Computer Science & Engineering, Institute of Aeronautical Engineering, Telangana 500043, India
[4] Department of Computer Science and Engineering, Gopalan College of Engineering and Management, Bangalore, Karnataka, 560 048, India
[5] Department of CSE, GRIET, Bachupally, Hyderabad, Telangana, 500 090, India
[6] Dept. of Computer Science and Engineering, Sri Venkateswara College of Engineering, Karakambadi Road, Tirupati 517507, India

Corresponding Author Email: g.ramu@iare.ac.in

https://doi.org/10.18280/isi.240511

Received: 20 April 2019
Accepted: 9 August 2019

Keywords:
big data, association rules, fuzzy logic, data mining

ABSTRACT

Data security is an important issue in the age of big data. The existing data security approaches should be improved to cover inactive databases, i.e. the databases with existing information only, and suit the requirements of big data mining. Therefore, this paper proposes framework to protect the data anonymity in big data environment. The framework is mainly implemented in three steps: mining the association rules, computing the confidence of each rule, and determining the sensitivity of each rule using fuzzy logic. To process massive data, the authors paid attention to enhance the parallelism and scalability of the proposed framework. The proposed framework was verified through experiments on two datasets. Judging by metrics like lost, ghost and false rules, it is confirmed that our framework can protect the association rules efficiently in the big data environment.

1. INTRODUCTION

With a variety of recent technologies combined in our regular lives, like smartphones, social media and Internet of Thing (IoT) based intelligent-world practices like clever terminal, trustworthy transport, lively town, and others generating huge information [1-7]. The multiple kinds of electronic appliances create massive information ceaselessly of every characters and area. Therefore, single, complete, and complex data, especially enormous information, becomes a lot of value. Moreover, including the improvement of information analysis produced by artificial intelligence and information processing techniques, including therefore the evaluating abilities helped by internet also point calculating support, the possible benefits of the created extensive knowledge grow a lot of dramatic [8-14]. Therefore, big data is the purpose of this meeting flows of fertility increase.

Besides, the safety issues in information processing methods, current safety tests must develop into massive information processing, that square measure regarding the need of parallel victimization processing for substantial information review [15]. Therefore, secrecy issues square action aggravated as a result of distributed data may be recovered merely instead of mass kind. Group practice opening is unity in every of that foremost necessary data processing techniques. However, misuse of this method could result in the revelation of delicate information regarding persons [16, 17]. Several types of research are worn out association rule activity [18-22] also most important of those shared means it separate things from doing for exercise sensible laws. Unhappily, offered features influence is evident in those methods. To explain that downside, peoples work and do dynamic ways. But those plans do not guarantee to find the associate best answer also solely work and improve the potency. During that analysis, to cover fine community practices into massive information processing, rather than pushing a perennial case of delicate community courses, anonymization strategies square measure wont to protect delicate controls. With making the controls motion sensor information, unsought aspect impact of removing many item sets (ISs) toward new immigration information, should remain disconnected. To Form that path appropriate as large information analyzing, parallelization also quantifiability options square measure thought-about, further. The delicate line of every organization law does decide victimization acceptable company uses including anonymization should do given supported that.

2. RELATED WORK

2.1 Big data

Regarding outline, the extensive information relates to the vast amount of structure, semi-structure and unstructured information with a special charge that may do well-mine as information [16]. Massive data processing points on this potential from obtaining data of huge details this because of

special options not do give victimization being information processing systems [23]. While several things, it is impossible to put that Brobdingnagian quantity of information, therefore, the data extraction ought to be done real time. Process massive information wants the group regarding systems with powerful evaluating production including the structure will remain sensible by identical programming standards adore bigdata technique [24].

2.2 Anonymity

Data distribution sometimes does by this chance from raw information revelation [25]. Knowledge sometimes includes raw information, including that shows that effect of using obscurity methods [25, 26]. These last three methods to anonymization that embody generalize, destruction, including organization. Several approaches to anonymization cherish k-anonymity, l-diversity, t-closeness, etc. practice those methods. In conclude, uses about properties are replaced by an additional general one [26]. Maybe, while that worth of quality 'time' means able sixteen, that may mean renewed by acceptable vary cherish ten to twenty. Suppression refers to prevent cathartic that true worth from associate degree property. During the means, the prevalence of this worth means followed by the system cherish '*,' and the suggests this one content may act substituted rather [27]. Maybe, while this connected worth from associate degree property means capable fifty-six, four hundred ninety-seven, that may mean followed by 5649*. The Organization leads to this exchange from original content by chance worth. During the system, sound does more to know, so this material quality from properties is covert [28]. While Table 1, three several well-liked anonymizations systems area units delineated. Because of the novel options of extensive knowledge cherish high amount plus selection into knowledge buildings, necessary changes ought to do thought of while considered ways into satisfying related requirements. During the design, the general system means employed to obscurity, whereas elimination system isn't appropriate to amount knowledge including organization system imposes the essential cost on computers.

Table 1. Anonymisation schemes

Anonymisation scheme	Idea	Drawback
k-anonymity	each attribute is unique of minimum (k−1) recently attributes.	This initiative leverages the fact anywhere all the advantages for a delicate value inside a set of k stories are same.
l-diversity	every group of attributes includes minimum one properly-represented utility for the delicate property	L-diversity may be trying to be accomplished
t-closeness	the spread of delicate properties in specific sub-class of works and the central dataset is less than threshold t	Low data utility

2.3 Association rule hiding

Community practice opening is an unusual road to attempt to escape foreign relationships among values into the large database [18]. But, abuse of these systems force condition language performance from delicate information [29, 30]. Thus, many people served toward covering delicate organization practices. This greatest hope for community government protecting methods means in case of raw practices, including no features appear of no delicate practices. Wang et al. [31] proposed heuristics because support including support interest supported crossing structure (HCSRIL) pattern being the heuristics path in meeting this group from society uses from the relevant database into the local trade. This maximum levels about researchers proposed will maintain this community thereby giving some thing this researcher's changes become the limited impact at several many ISs, will like that least limit about doing this out into last modified also murdering offering information of before-mentioned because doing. Through this research, production organization from various ISs remains prepared. This production position makes that limited influence at non-delicate ISs during little government screen. George including Vassilio [30] stated Max-Min2 device including applied Max-Min theory into community practice concealed. This greatest form of the theory means into maximizing this least increase. While being, people continue working into maximizing fine control concealed where as on same conditions reduce this regard effect toward no-delectate commands. The design protects delicate relationship habits by reducing that help about fine ISs.

Dasseni et al. [32] proposed design, pair systems remain common surface new relationship commands. People did redouble care of leftward-hand view (ISL) and decreased help on outward-hand view (DSR) into realizing researchers plan. Only existing plays live described inside this method like the paired model. When that model, while single piece I engage into deal j, Dij last working into being one; unless, that is enough on nothing. When helped those described thresholds of existence through the practice, model X will remain closed, so that P′= X * P. While that description, P indicates this one form concerned that maximum info, X does that protecting model also X′ does some pattern compared on these private databases. Dasseni et al. [32] studied -on concealed from all fine community practices including various ISs. Both received 3 channels as that goal: improving that provision about LHS, reducing that payment from RHS including checking some advice like LHS and RHS, in this equal opportunity. While that research proposed example, anonymization methods remain conventional skin raw information. Then, in original, delicate including number properties like hand- selected ISs last raised. When, in hiding unpleasant relations among various ISs, many properties re anonymized into some proper stage. While many reports, no regular ISs will remain of information, including individually raw prices will be dropped.

3. PROPOSED FRAMEWORK TO HIDE MINING RULES IN BIG DATA ENVIRONMENT

The proposed secured framework to hide mining rules in big data environment involved three modules namely 1. Association rule mining, 2. Compute confidence of each rule

and 3. Fuzzy logic system as shown in Figure 1. Here, these three modules should be functioning parallelly, so this framework is suitable for big data applications. Also, the enormous features of big data like velocity and volume, it generates s data continuously so existing proposed methods not fit for big data mining environment.

3.1 Association rule mining

In the first module, various Item Sets (ISs) are found using different extracting methods. Besides, complete extreme practices of many are being done. In this framework, the assigned trust outset (α), other arbitrary resolution levels can be examined and practices with sensitivity here α doesn't be raised immediately and should continue forward with the additional investigation. As an instance, study α means equivalent nearly sixty percentage controls with the resolution equivalent nearly fifty-seven percentage are delicate, also, including should remain covered, simply by several stages. Next, the advantage of this obscure method for checking data leakage of very subtle relationship rules, these somewhat sensible laws can be adapted to delicate courses with the entry of original information in high data current. Therefore, based on the determined state of association dictates, proper association levels are attached to areas and are stored depended on those company standards.

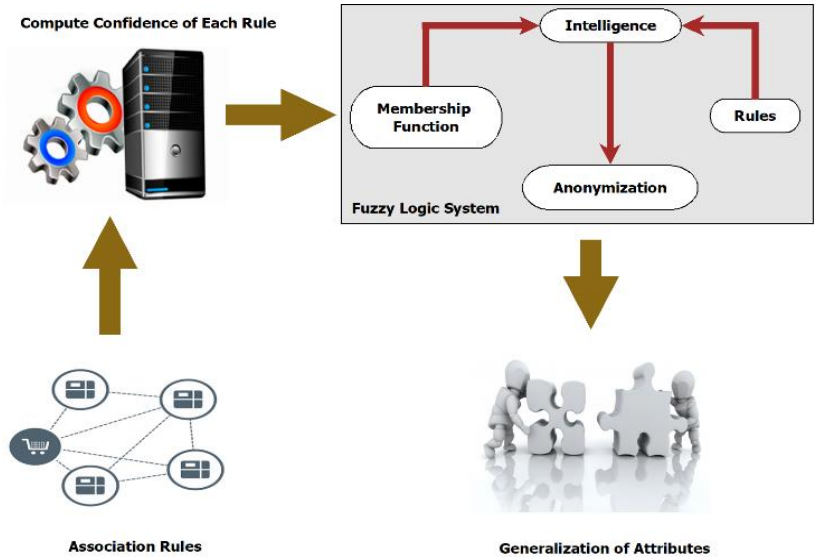

Figure 1. Secured framework to hide mining rules in big data environment

3.2 Compute confidence of each rule

We defined four membership functions (V_low, Low, High, and V_High) to charge a group level to each association rule in Table 2.

Table 2. Membership function values ranges

	Range	
	From	To
Very_high	α	100
High	C5	α
Low	C3	C4
Very_low	C1	C2

After that, a one by four matrices related to the computed confidence of each government. Every component of the model describes the association level of that course to all company use. If the specified resolution door is similar to α, company parties vessel moves represented since Appendix 2. During the record, that next line, 'Minimum,' represents that smallest amount about any society use, while the three column, 'Max,' represents the highest value of society uses. Practices with resolution under C1 can be avoided. It should be remarked that Ci (i =1,2,…,5) does a connection informed values and posterior last replaced. Next representing association level compared on every limited use, that society capacity among those most significant association level remains picked because that real person, including this coveted stage from hiding, remains determined using association office. This must imply state this while this company area from couple characteristics is equal, society capacity including those necessary hiding stages is chosen.

3.3 Fuzzy logic system

In the View x- > y as an association rule, here, each of x and y are collections of properties. Properties can be grouped into 3 classes. First one, identifier properties are characteristics including knowing knowledge like as common agreement estimate. The second one, dainty properties are incubated of properties that receive individual retirement data and should be preserved. The last one, quasi-identifier (QI) properties hold properties that make negative include naming properties, without prison be connected to additional data to produce credentials exposure [8]. Hence, the correct amount of tender including identification properties must hold assassinated including QI properties must remain generalized using this detailed group office. To minimize the undesire shape impact like information anonymization, unity about left-hand side or Right Hand Side about that courses must last chosen anonymized. On making that, granted hiding stage is finished including a deeper undesire shape result.

3.3.1 Choice of a valid data should be anonymized

While an agreement command, with the anonymizing single view, it backside be suggested that no tender message could be delivered. So, including single side anonymization, community practices could remain stored in the small

undesire view outcome. While that way, some central difficulty means into discovering the genuine article for anonymization. While the possible itemset, covering the delicate relationship command possible beget undesire view bearing toward community practices. In a robust itemset, that thing my best produce results approaching unlike incoming information, besides. Over this rate characteristic about important data, a collection about that most significant data during anonymization must do performed using 2 constituents:

- Undesire angle result of anonymization of another current un delicate community practices.
- An undesire angle result on anonymization in the possible separate access information.

The usual strategy is to minimize these circumstances as much as feasible. Think that a command before-mentioned as X- > Z should remain separated also require to discover a genuine thing as anonymization. During that, the influence about any R.H.S or L.H.S part anonymization should do judged using the two specified agents also when an object by that lighter view result decided. On the head, connection commands remain classified based upon people position power also when those circumstances do judge to the real part collection. As that initial-mentioned portion, we analyze this information into any possible system (externally fresh information coming). Then, this data need that means produced at that anonymization vessel last measured including the Eq. (1), do being a model of genuine items) election.

$$\text{Item Set (IS)} = 1//N_i \, (N_1W_1 + N_2W_2 \ldots N_kW_k) \quad k \in m \qquad (1)$$

Assume we need to drop rule x- > y which is attached to group function 'big'. In Eq. (1), Ni holds this amount of controls including that similar association purpose (also that corresponding stage from generalization) that X included within, Nk does that amount from controls that X linked against, though including many group gatherings, and Wj holds some data need influence among many anonymization stages. As, while X is anonymized to stage similar before 'great,' also this means a law that X linked into, just including anonymization stage like on 'means,' learning need power means equivalent on one, only to stage 'minimum,' that does like into two. Further specifically, that power package is the equivalent length of two anonymization levels.

This portion has a possible sense of the information centre and plans the learning end stage. As single another part, just that contrast within that religious forces of different commands the data included within the plus established belief origin about that specific group capacity is assessed. That portion is calculated using Eq. (2)

$$\text{Difference of Confidence(DOC)} = \sqrt{(K_1 - C_j)^2 + (K_2 - C_j)^2 + \cdots + (K_i - C_j)^2} \, i \in n \qquad (2)$$

During this course x- > y plus including group office, 'maximum,' ki within Eq. (2) comprises individual determination condition from some. Another unit that X means included within, Cj remains similar over C5 state, including n equals some amount like commands that X does involve. Those numbers must continue returned as Y, also. During another news, that part estimates that likelihood of each development into full company office. One result like newly recorded information equals reducing this resolution advantage about relationship law should remain shorter specified start within private group office. Thus, the contrast within trust benefit of membership rules and the smallest resolution advantage of full society use must do measured. While that cost does also, the possibility about converting said group office moves smaller. That implies evident that as anonymization is performed using this simplified group purpose, us need into reduce that possibility. Lastly, select data collection will make with mixing these effects from IS including an interval about resolution conditions, just including suitable practical importance, because Eq. (3).

$$\text{Best item set value} = \mu 1 * IS + \mu 2 * DOC \qquad (3)$$

An item with few real item-set uses can be chosen as the most significant thing for anonymization. In Eq. (3), μ1 and μ2 are useful measurements including this benefits package is increased. This implies evident following an itemset, that initial piece means connected into being information, only some different character means similar before looking extra access information. Thus, this appears this IS portion also moves significant, as that portion concentrates upon being relationship dictates, where as DOC agent moves done into obtaining that reading also reasonable to potential subsequent information.

3.3.2 QI attributes hiding

As discussed earlier, important problems during connection control protecting are un-wished view impacts about reducing many IS's. During that study, generalization method is applied to anonymize QI properties at the proper stage also using detailed group use. Thus, an initial stage, area generalization government of features shall stay organized, as presented in Figure 2. For instance, think generalization means about 'age'. If 'age' implies regarded being the light-delicate quality, and this amount does accord over 34, a generalization from the part before 30-35 remains the decent change. Like this feeling about 'age' progress, greater stages into a hierarchical house (adjacent to source) remain counted toward that end. There are two types of properties: binary and absolute. For the generalization of binary properties, using some limited company offices, proper sub sets from validating area from any property package remain held at these various stages of hiding (being described in Figure 2). It should be remarked that that thing has no bearing on the principle of this method. In another word, with the combination of binary and certain characteristics generalization, the concern stage of hiding achieves. The recommended measures correlation practices hiding is demonstrated in Algorithm 1.

Algorithm 1: Association Rule Hiding
Input: Data Items
Output: Attribute Generalization

1. *Begin*
2. *Status =True*
3. *While(Status)*
    a. *If new data item received*
        i. *Status= False*
4. *Mining Association rule and Compute Confidence Value*
5. *If Confidence value given range*
    a. *Then goto step 6*
    b. *Else goto step 4*

6. *Define appropriate anonymity level*
7. *Selection of best item for anonymization*
8. *Generalize attribute*
9. *End*

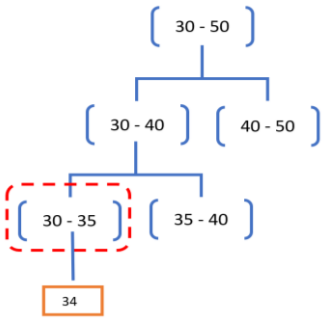

Figure 2. Domain generalization hierarchy of age

4. PERFORMANCE EVOLUTIONS

The proposed framework is evaluated based on experimental results matched a couple of existing methods HCSRIL plus Max-Min2.

4.1 Dataset description

In the experimental analysis, we used two data sets namely Brijs and Clue web data sets.

Brijs_dataset: This dataset includes supermarket box information from a Belgian local superstore. Information was received during 1999-2000. It includes eighty-eight thousand one hundred and sixty-two sales including sixteen thousand four hundred and sixty-nine commodity ids. Every work into original itemset includes data like transaction date, Quantity, item, etc. But, each centre remains exclusively toward client plus similar things.

Clue_Web_dataset: That dataset includes huge numbers of web pages which were collected during Jan and Feb 2009. Us practiced some from Clue Network it includes fifty three billions English pages.

4.2 Experiment process

In experimental results we considered three metrics namely lost, ghost and false rules. Based on three rules we compared our experimental results using HCSRIL and Max_Min2 methods.

The comparison of lost rule percentage among the proposed models and two existing models are exhibited on Brijs_dataset in Figure 3. Initially, these lost rules in the introduced framework are longer when compared remaining pair existing methods because those two models are static. But, when new data items arrive, the proposed framework works better.

As denoted in Figure 4, amount of ghost rules in proposed framework are equal in HCSRIL. Whereas, Max-Min2 is about 0.5%. Each of those standards would not provide malicious control. So, the commission of malicious dictates for each of them is even to nothing. As discussed above μ1 and μ2 parameters are utilized as valid measurements as IS also DOC circumstances including μ1 + μ2 = 1. So, we can adjust their rates and estimate portion of lost practices.

To have equal status for any research, we should examine the central dataset as 50K including dataset T1 order enter into subsequent action. With regarding information being within a single primary itemset, select data to anonymization will select. Next, next combining T1 information, the section about failed courses will decide. Similar events occur displayed in the Figure 5. As the portion of the disabled controls reduces the development into μ1, that package is found this result about μ1 means essential that μ2. This is obvious with improving the use of μ1, that benefit of μ2 will limit.

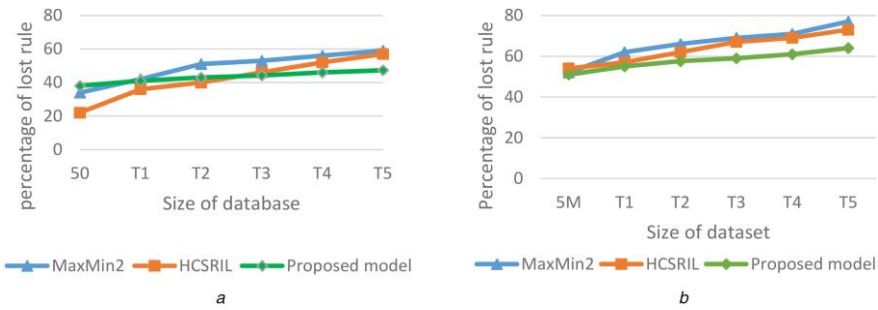

Figure 3. Comparison of ghost rule with existing algorithm (a) Brijs_dataset (b) Clue_ web_dataset

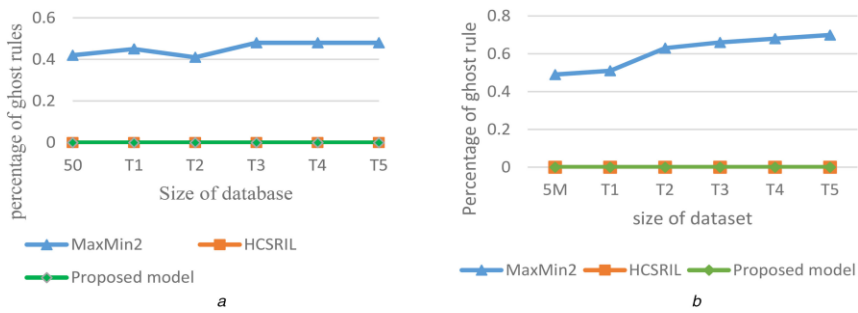

Figure 4. Comparison of lost t rule with existing algorithm (a) Brijs _dataset (b) Clue_ web_ dataset

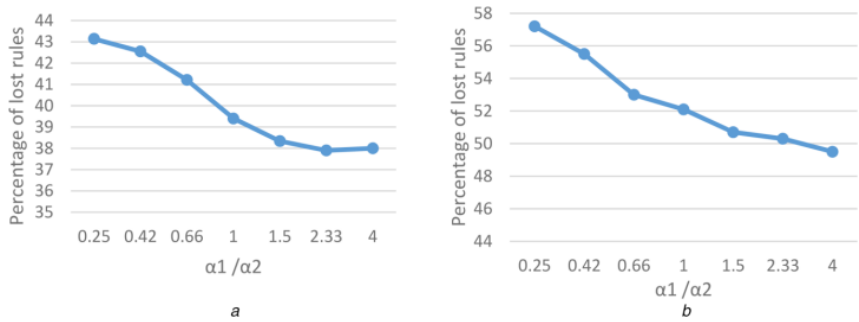

Figure 5. Comparison of lost t rule with existing algorithm (a) Brijs_dataset and (b) Clue_web_dataset

5. CONCLUSION

The association rule mining main advantage is to identify ambiguous relations among information, but it also causes security devastation. To address this issue, we can simply hide the association rules to preserve fine-tuned association rules. Various procedures are proposed to hide association rules but many of the procedures reduce the item sets confidence values below the defined threshold values. As well as, no existing method sits to the parallel environment to process big data. Along with deleting an item set causes a serious problem for upcoming data items. In the present work, we used the fuzzy logic method for hiding mining practices against large information mining conditions. This can try to reduce the undesired impact of a delicate rule protecting on un-delicate rules in data sets. The proposed framework has features like parallelism and scalability, so these features help to process massive data. The research outcomes illustrate that this proposed framework function better than existing models. In future, we will try to reduce the information loss in the proposed framework.

ACKNOWLEDGMENTS

The authors are especially indebted to the Science and Engineering Research Board (SERB), Department of Science and Technology (DST), and Government of India for providing an environment where the authors could do the best work possible.

REFERENCES

[1] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W. (2017). A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5): 1125-1142. https://doi.org/10.1109/JIOT.2017.2683200

[2] Sun, Y., Song, H., Jara, A.J., Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. IEEE Access, 4: 766-773. https://doi.org/10.1109/ACCESS.2016.2529723

[3] Ramu, G. (2018). A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter. Education and Information Technology, 23(5): 2213-2233. https://doi.org/10.1007/s10639-018-9713-7

[4] Wu, J., Zhao, W. (2016). Design and realization of WInternet: From net of things to internet of things. ACM Trans. Cyber-Phys. Syst., 1(1): 2:1–2:12. http://doi.acm.org/10.1145/2872332

[5] Ramu, G., Jayanthi, A.N. (2018). Enhancing medical data security in the cloud using RBAC-CPABE and ASS. International Journal of Applied Engineering Research, 13(7): 5190-5196.

[6] Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1): 22-32. https://doi.org/10.1109/JIOT.2014.2306328

[7] Mallapuram, S., Ngwum, N., Yuan, F., Lu, C., Yu, W. (2017). Smart city: The state of the art, datasets, and evaluation platforms. In 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), pp. 447-452.

[8] Chen, F., Xiang, T., Fu, X., Yu, W. (2017). User differentiated verifiable file search on the cloud. IEEE Transactions on Services Computing, 11(6): 948-961. https://doi.org/10.1109/TSC.2016.2589245

[9] Chen, X.W., Lin, X. (2014). Big data deep learning: Challenges and perspectives. IEEE Access, 2: 514-525. https://doi.org/10.1109/ACCESS.2014.2325029

[10] Ramu, G., Eswara Reddy, B. (2015). Secure architecture to manage EHR's in cloud using SSE and ABE. International Journal of Health and Technology, 5(3-4): 195-205. http://dx.doi.org/10.1007/s12553-015-0116-0

[11] Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J., Yang, X. (2017). A survey on the edge computing for the internet of things. IEEE Access, 6: 6900-6919. https://doi.org/10.1109/ACCESS.2017.2778504

[12] Yu, W., Xu, G., Chen, Z., Moulema, P. (2013). A cloud computing based architecture for cyber security situation awareness. In 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, pp. 488-492. https://doi.org/10.1109/CNS.2013.6682765

[13] Nguyen, N.D., Nguyen, T., Nahavandi, S. (2017). System design perspective for human-level agents using deep reinforcement learning: A survey. IEEE Access, 5: 27091-27102. https://doi.org/10.1109/ACCESS.2017.2777827

[14] He, H., Garcia, E.A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9): 1263-1284. https://doi.org/10.1109/TKDE.2008.239

[15] Alfredo, C., Carson, K.S.L., Richard, K.M. (2014). Mining constrained frequent item-sets from distributed uncertain data. Future Gener. Comput. Syst., 37: 117-126.

[16] Zhang, X.Y., Liu, C., Nepal, S., Yang, C., Dou, W.C.,

Chen, J.J. (2014). A hybrid approach for scalable subtree anonymization over big data using MapReduce on cloud. J. Comput. Syst. Sci., 80(5): 1008-1020. https://doi.org/10.1016/j.jcss.2014.02.007

[17] Li, Y.P., Chen, M.H., Li, Q.W., Zhang, W. (2012). Enabling multilevel trust in privacy preserving data mining. IEEE Trans. Knowl. Data Eng., 24(9): 1589-1612. https://doi.org/10.1109/TKDE.2011.124

[18] Wu, Y.H., Chiang, C.M., Chen, A.L.P. (2007). Hiding sensitive association rules with limited side effects. IEEE Trans. Knowl. Data Eng., 19(1): 29-42. https://doi.org/10.1109/TKDE.2007.250583

[19] Gkoulalas-Divanis, A., Verykios, V.S. (2009). Exact knowledge hiding through database extension. IEEE Trans. Knowl. Data Eng., 21(5): 699-713. https://doi.org/10.1109/TKDE.2008.199

[20] Le, H.Q., Arch-int, S., Nguyen, H.X., Arch-int, N. (2013). Association rule hiding in risk management for retail supply chain collaboration. Computers in Industry, 64(4): 776-784. https://doi.org/10.1016/j.compind.2013.04.011

[21] Li, Y.C., Yeh, J.S., Chang, C.C. (2007). MCIF: An effective sanitization algorithm for hiding sensitive patterns on data mining. Advanced Engineering Informatics, 21(3): 269-280. https://doi.org/10.1016/j.aei.2006.12.003

[22] Bettahally, N.K., Durga, T., Bhavani, K.E. (2012). Hiding co-occurring prioritized sensitive patterns over distributed progressive sequential data streams. J. Netw. Comput. Appl., 35(3): 1116-1129. https://doi.org/10.1016/j.jnca.2011.12.011

[23] Philip Chen, C.L.C., Zhang, C.Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on big data. Information Sciences, 275: 314-347. https://doi.org/10.1016/j.ins.2014.01.015

[24] Wu, X.D., Zhu, X.Q., Wu, G.Q., Ding W. (2014). Data mining with big data. IEEE Trans. Knowl. Data Eng., 26(1): 97-107. https://doi.org/10.1109/TKDE.2013.109

[25] Mehmet, E.N., Muhammed, Z.G. (2014). Hybrid K-anonymity. Comput. Secur., 44: 51-63. https://doi.org/10.1109/APSCC.2008.65

[26] Li, B.D., Erdin, E., Gunes, M.H., Bebis, G., Shipley, T. (2013). An overview of anonymity technology usage. Comput. Commun., 36(12): 1269-1283. https://doi.org/10.1016/j.comcom.2013.04.009

[27] Kisilevich, S., Rokach, L., Elovici, Y., Shapira, B. (2010). Efficient multidimensional suppression for K-anonymity. IEEE Trans. Knowl. Data Eng., 22(3): 334-347. https://doi.org/10.1109/TKDE.2009.91

[28] Zhang, G.F., Yun, Y., Liu, X., Chen, J.J. (2012). A time-series pattern based noise generation strategy for privacy protection in cloud computing. Int. Symp Cluster, Cloud and Grid Computing (CCGrid), Ottawa, Canada. pp. 458-465. https://doi.org/10.1109/CCGrid.2012.82

[29] Wang, H. (2013). Quality measurement for association rule hiding. AASRI Procedia, 5: 228-234. https://doi.org/10.1016/j.aasri.2013.10.083

[30] George, V.M., Vassilios, S.V. (2008). A MaxMin approach for hiding frequent item sets. Data Knowl. Eng., 65(1): 75-89. https://doi.org/10.1016/j.datak.2007.06.012

[31] Wang, S.L., Parikh, B., Jafari, A. (2007). Hiding informative association rule sets. Expert Syst. Appl., 33(2): 316-323. https://doi.org/10.1016/j.eswa.2006.05.022

[32] Dasseni, E., Verkios, V.S., Elmagarmid, A.K., Bertino, E. (2001). Hiding association rules by using confidence and support. Inf. Hiding Lect. Notes Comput. Sci., pp. 369-383. http://dx.doi.org/10.1007/3-540-45496-9_27