View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Directory of Open Access Journals

Journal of Universal Computer Science, vol. 25, no. 3 (2019), 270-281
submitted: 28/3/18, accepted: 30/12/18, appeared: 28/3/19 © *J.UCS*

Combination Model of Heterogeneous Data for Security Measurement

Xiuze Dong
(Department of Electronics and Communications Engineering
Beijing Electronic Science and Technology Institute, Beijing, China
dongxz@besti.edu.cn)

Yunchuan Guo
(Institute of Information Engineering, CAS, Beijing, China
guoyunchuan@iie.ac.cn)

Fenghua Li*
(Institute of Information Engineering, CAS, Beijing, China
School of Cyber Security, University of Chinese Academy of Sciences, China
lifenghua@iie.ac.cn
*Corresponding author)

Liju Dong
(Faculty of Engineering and Information Sciences
University of Wollongong, Wollongong, NSW 2522, Australia
liju@uow.edu.au)

Arshad Khan
(School of Computer, Engineering and Mathematics
Auckland University of Technology, New Zealand
Arshidkhan1991@gmail.com)

Abstract: Measuring security is a core step for guaranteeing security of network and information systems. Due to massiveness and heterogeneity of measurement data, it is difficult to classify and combine them on demand. In this paper, considering implication relationship of metrics, we propose a combination model and combination policy for security measurement. Several examples demonstrate the effectiveness of our model.
Key Words: security measurement, data combination, heterogeneous data
Category: H.2.1, H.2.5, E.2

1 Introduction

Security measurement for network and information systems [Yu et al., 2018], used to evaluate the ability of protecting security in the real operating environment and involving security technology, management, manipulation and other

aspects, is a significant step to ensure system security. Obviously, ignoring security measurement will suffer from severe consequences. According to Kaspersky Lab, in 2017 [1], attackers used a vulnerability in the Apache Struts 2 framework and stole the data of 145.5 million people and compromised more than 209,000 credit card numbers, including clients names, social security numbers, dates of birth, and addresses.

According to BBC news [2], Ukraine has suffered two hacks on its power grid, one in 2015 and the other in 2016. The first affected 225,000 and the second knocked out about one-fifth of Kiev's power consumption.

One of key reasons for the above events is lack of accurate measurement for information systems. Due to this lack, the elements that effect information security can not be correctly recognized and the interior states cannot be effectively analyzed. Thus, it is impossible for us to prevent attacks or decrease attack possibility. In fact, security is impossible without security measure.

To accurately measure security, we should classify and combine measurement data on demand for the following reasons: security metrics for a system rely on its security requirements and data with different categories should be taken as evaluation input to evaluate each metric. For example, in the military application, confidentiality is more cared about, thus data related to information leakage should be taken as an evaluation input; In the life-critical scene, availability and integrity are more cared about, thus data related to resource consumption and pollution might be required; In cloud scenarios [Yu et al., 2017, Li et al., 2019, Xue et al., 2019], availability and privacy are preferred. In practise, even for the same security metric, data category used for evaluation is different. For example, for the confidentiality measure, data used in military scene are different from the person scene. However, it is difficult to classify and combine data on demand due to data massiveness and heterogeneity[3] and several challenges exist, as follows.

(1) Data division for security measure. Generally, one type of data can be described by several dimensions. For example, in the real-world web image database from National University of Singapore, an image is labeled using 1,134 dimension feature vector including 500-D bag of words [4]. The tags2con dataset, manually created by a group of human annotators owns 500 user-bookmarks pairs. Obviously, it is very difficult to directly use these dimensions to measure security. It

[1] https://www.kaspersky.com/blog/data-leaks-2017/19723/

[2] $https://www.bbc.com/news/topics/cp3mvpdp1r2t/cyber-attack\&link\_location=live-reporting-story$

[3] According to Forbes, data created by human society will hit 163 Zettabytes in 2025. These data, which come from a large number of management domains, security domains and application systems, are often massive and heterogeneous. https://www.forbes.com/sites/andrewcave/2017/04/13/what-will-we-do-when-the-worlds-data-hits-163-zettabytes-in-2025.

[4] https://lms.comp.nus.edu.sg/research/NUS-WIDE.htm

is a huge challenge for us to dividing data from the aspect of security measure.

(2) Combination policy. Because data from a large number of sources are often heterogeneous and massive and they can't be directly used for measuring security. Due to variation of security metrics, it is different for us to design one policy to combine heterogeneous data.

To address the above challenges, in this paper, we propose a combination model of heterogeneous data for security measurement. Our main contributions are as follows.

(1) Considering implication relationship of metrics, we design hierarchical metrics graph (HMG), including three layers: property layer, event layer and data-collection-item layer. Based on the HMG, we present a fine-grained division scheme to classify evaluation data for security measure.

(2) Based on HMG, a series of combination policies for measuring security are proposed, including time-based priority, majority-based priority and low-risk priority policies. Several examples demonstrate the effectiveness of our scheme.

The rest of this paper is organized as follows. In Section 2, we discuss the related work. In section 3, we propose our model to combine heterogeneous data. We draw a conclusion in section 4.

2 Related work

Through data combination, data from multiple sources are integrated to produce more consistent and trust information than that provided by an individual source. Roughly, data combination, widely used for multi-sensor [Khaleghi et al., 2013], privacy [Komarova et al., 2018], and disaster detection[Ghosh, 2017], can be divided into three categories [Zheng, 2015, Khaleghi et al., 2013]: the data-level-based combination, the feature level-based data combination, and the decision-based data combination.

In the first approach, algorithms for data combination, taking raw data gathered from different data sources as input and producing more reliable and accurate data, can be divided into two categories: concatenation-based combination and fusion-based combination. In the concatenation-based scheme, multiple datasets are loosely and simple coupled, without considering their consistency, correlation and disparateness. For example, combining the POIs (points of interest) from several regions, we can obtain all POIs of a city.

In the fusion-based combination, when data are combined, data inconsistency, data correlation, data imperfection and disparateness should be tackled. Along with this scheme, Angelov et al. [Angelov and Yager, 2013] proposed a new data fusion operator based on averaging to cluster and classify data. Dong et al. [Dong et al., 2014] designed a self-adaption scheme with weighted average to combine multiple data with different precision and enhance combination precision. Graham et al. [Graham et al., 2016] proposed a local estimator

to possess a double robustness property and classify semiparametric data. To combination privacy data, based on infrequent observations, Komarova et al. [Komarova et al., 2018] proposed a series of data combination rules and accurately formalized combination conditions. Considering the identification of counterfactual distributions, Fan et al.[Fan et al., 2014] adopted both the conditional independence assumption and the common support assumption, and proposed treatment effects under data combination.

In the feature-level-based combination, multiple features, treated equally or unequally, are combined into feature vectors. In the *equivalence* scheme, several features are concatenated sequentially [Wang et al., 2014]. However, this approach can cause the over-fitting, redundancy and dependency problems [Zheng, 2015]. To address these problems, machine learning (e.g., convolutional neural networks [Chen et al., 2016, Romero et al., 2016], recurrent neural network [Du et al., 2015], deep autoencoder [Xing et al., 2016] and deep belief network[Jang et al., 2017]) are proposed to extract and fuse features.

Using a convolutional neural network, Chen et al. [Chen et al., 2016] proposed a regularized feature extraction scheme to accurately classify hyperspectral image. Romero [Romero et al., 2016] designed single-layer and deep convolutional networks to remotely analyze sensing data and used greedy layerwise unsupervised pertaining to learn sparse features. Shao et al.[Shao et al., 2017] developed an enhancement scheme of deep feature fusion to rotate machinery fault diagnosis. Charte et al. [Charte et al., 2018] surveyed autoencoders for nonlinear feature fusion from the aspect of taxonomy, models, software and guidelines. Considering recurrent neural network, Du et al. [Du et al., 2015] proposed an end-to-end hierarchical RNN for skeleton based action recognition. Cascading 3-dimensional CNNN, Nguyen et al. [Nguyen et al., 2018] introduced deep spatio-temporal features to recognize multimodal emotion.

In the decision combination, depending on specific fusion criterion, serval sub-decisions from several individuals are combined into the optimal decision [Hall and Llinas, 1997]. Roughly, decision fusion can be divided into three categories: Bayesian inference[Chen and Varshney, 2002], Dempster-Shafer evidence theory [Kuncheva et al., 2001] and fuzzy theory[Fatemipour et al., 2014].

Using Bayesian inference, Chen et al.[Chen and Varshney, 2002] reformulated decision fusion problem as hierarchical models and proposed a Gibbs sampler to perform posterior probability-based fusion. However, this approach cannot distinguish between uncertain and unknown information. To address this problem, Fontani et al. [Fontani et al., 2013] and Zhang et al. [Zhang and Ge, 2015] used Dempster-Shafer evidence theory to combine decision for image forensics and for fault detection, respectively. Using fuzzy theory, Ribeiro et al. [Ribeiro et al., 2014] designed a fusion algorithm based on multi-criteria decision making.

Although a large number of efforts are spent on data combination, no one combines data from security measure. In this paper, we propose a combination model of heterogeneous data for security measure.

3 Combination Model for Heterogeneous Data

3.1 Classifying Heterogeneous Data Using Hierarchical Metrics Graph

In this subsection, we define hierarchical metrics graph and then use it to classify heterogeneous data for security measure. To achieve this goal, we first give the definitions used in sequel.

Definition 1 *(Metrics Graph, MG). Metrics graph $MG = (V, E)$ be a weighted and directed acyclic graph, where $V = \{v_1, \ldots, v_n\}$, a set of vertex, denotes all metrics for security evaluation; Vertex can be divided three layers: property layer, event layer and data-collection-item layer. A property layer is composed of property nodes, which denote the security properties that network and information systems should satisfy. An event layer consists of a set of event nodes. If the event in an event node happens, then the corresponding property for this node will be compromised. Nodes in the data-collection-itme layer are used to label the required collection data for detecting the event which connects this node. For example, to violently crack password, an attack has to continuously and repeatedly guess the used password. If the login password for the same account continuously and repeatedly fails, then event violent cracking might happen. In this case, data item of incorrect password should be collected to detect the violent cracking event.*

$E \subseteq V \times V$, a set of edges between nodes, denotes the hierarchy relationship between metrics. Assume that $e = (v_1, v_2)$ is an edge of graph MG, we have the following constrains.

- *if both v_1 and v_2 are property nodes, then property v_2 is a sub property of v_1;*
- *if v_1 and v_2 are a property node and an event node, respectively, then the property denoted by v_1 will be violated when event denoted by v_2 happens.*
- *if both v_1 and v_2 are event nodes, then one of the pre-conditions of event v_1 is the occurrence of event v_2.*
- *if v_1 and v_2 are an event node and an data-collection-item node, respectively, then the data denoted by v_2 should be collected for detecting the event denoted by v_1.*

Generally, security properties can be divided into two categories: basic properties and extended properties. According to definition of information security proposed by Fang [5], there are four basic properties : confidentiality, authentication, availability and controllability. Both events can bring a positive or negative impact on security properties. For example, encryption has a positive impact on confidentiality and weak password has a negative impact on confidentiality. To distinguish the two impacts, symbols + and - are used to denote the positive and negative impacts on security property.

Definition 2 *(Hierarchical Metrics Graph, HMG): Given metrics graph MG with weight W (*i.e., $HMG = (V, E, W)$*), HMG is a hierarchical metrics graph, if the following conditions are satisfied:*

(1) In graph MG, there exists only one node with the zero *in-degee . This node is called the root node of HMG;*

(2) Given two edges $e_1 = (v_{11}, v_{12})$ *and* $e_2 = (v_{21}, v_{22})$ *of graph MG, if* $v_{12} = v_{21}$*, then* (v_{11}, v_{22}) *is not in edge set E (i.e.,* $(v_{11}, v_{22}) \notin E$*);*

(3) Given property node v, the set of its sub property-nodes $\{v_1, v_2, \cdots, v_n\}$ *and the set of the corresponding out-edges* $\{e_1, e_2, \cdots, e_n\}$ [6] *, weight* $w_i (0 \leq w_i \leq 1)$ *is assigned to edge* e_i *with constrains* $w_1 + \cdots + w_n = 1$*. This weight denotes the importance of property* v_i *to property v.*

Given edge $e = (v1, v2)$ of HMG, the hierarchy of its starting node (i.e., v_1,) is always higher than that of its ending node (i.e., v_2).

According to Fang [7], we can give the HMG for security measurement, as shown in Fig 1. According to this definition, four basic properties (i.e., confidentiality, availability, controllability and authentication) can be used to measure security, where reliability, stability and survivability are sub-properties of availability. In Fig. 1, weights ω_1, ω_2, ω_3, ω_4 denote the importance of availability, confidentiality, controllability and authentication to security measurement in a specific scene. For example, in a scene, if availability, confidentiality and authentication are equally important, and controllability can be ignored, then we can set $\omega_1 = \omega_2 = \omega_4 = \frac{1}{3}$ and $\omega_3 = 0$.

According to HMG and requirement for measuring security of the specific scene, we can divide heterogeneous data into several categories. For example, if we only consider the availability, then data, used to label leaf nodes whose ancestor is availability, can be regarded as one category; the other data can be ignored because these data do not be used to measure availability. Algorithm 1 shows how to classify data using HMG.

[5] https://wenku.baidu.com/view/00b08709bb68a98271fefa55.html
[6] That is, $e_1 = (v, v_1), \ldots, e_n = (v, v_n)$
[7] http://blog.sina.com.cn/s/blog_7110463b0100ynty.html

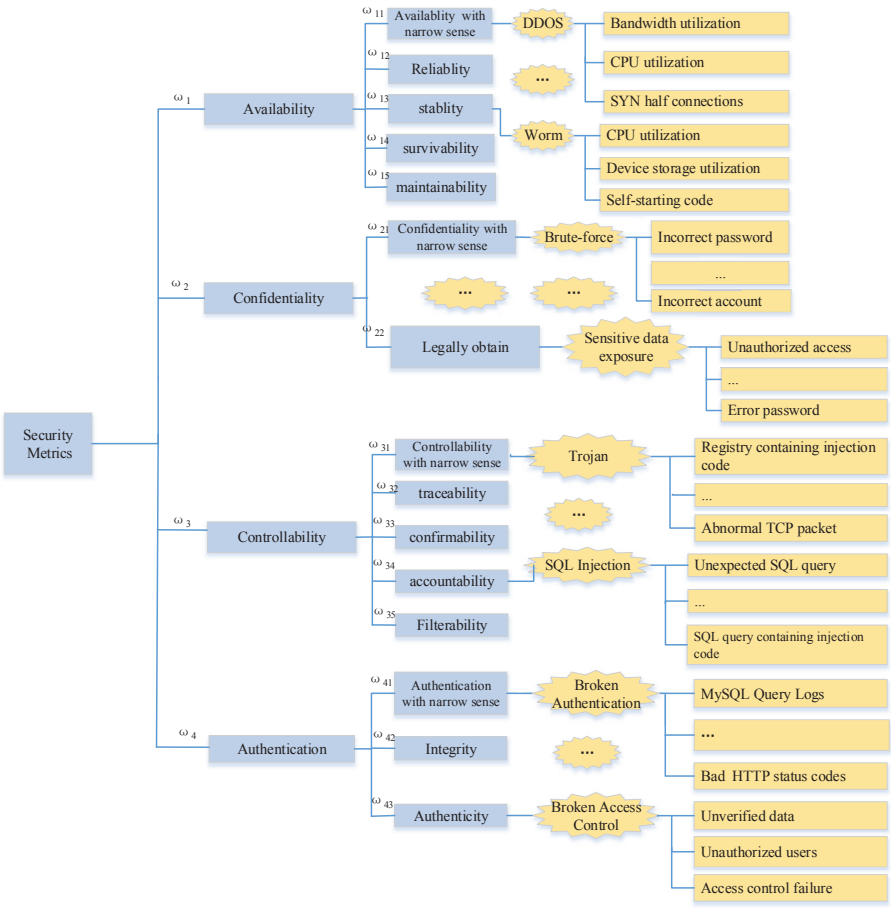

Figure 1: Example: Hierarchical Metrics Graph

3.2 Combining heterogeneous data

After classifying data, we should consistently combine these data. Generally, the combination schemes can be roughly divided into two categories: physical combination and logical combination. Physical combination denotes that more than one piece of data are piled up, including: the file-level combination, the tuple-level combination, the database-level combination, the table-level combination, the row-level combination and the column-level combination. In logical combinations, more than one piece of data are fused into one organic whole. However, during the data combination, the following challenges exist.

Data consistence: Data, used to measure security, come from a large num-

Algorithm 1: Classify data using HMG

```
Input: Security goal; data to be classified; HMG
Output: Classification of the queried data
Querys the queried security goal from HMG and returns the corresponding node ;
Takes the returned node as the root node and starts to traverse the sub-HMG (note: the
returned is the root of the sub-HMG) ;
while Traversing sub-HMG is NOT completed do
    if Data to be queried match a leaf node then
        Adds the label of the node to the queried data ;
    end
end
```

ber of data sources and are inconsistent. For the same leaf metric shown in Fig. 1, its values from the different data sources might vary. For example, in cooperative intrusion detections, to detect whether an intrusion even happens in a system, multiple nodes cooperatively monitor the detected system and report their monitor results. However, the capabilities of nodes vary. This will cause inconsistent results. To accurately detect an intrusion event, it is necessary to consistently combine data from different data sources.

Data heterogeneity: Data (e.g., log information, and device information) collected by collection agent are often semi-structured and even heterogeneous. Obviously, a measurement system cannot take heterogeneous data as input. Thus, we should converse semi-structured or heterogeneous data to structured data.

3.2.1 Consistence guaranteeing

In this subsection, we discuss composition policies that can be used to guarantee data consistence.

Policy 1 *(Time priority): If more than one piece of data are labelled to one leaf node in HMG, then the latest piece of data is selected as the final result.*

Example 1 *Assume that there are two firewall logs as shown in Fig. 2, the first log and the second log happen at Aug 24 2017 08:54:48 and Jan 13 2014 13:46:36, respectively. After the two logs are combined, the combination result is the first log and the second log can be ignored (because the second log is out of date).*

Policy 2 *(Majority priority): If more than one piece of data are labelled to one leaf node in HMG and then the piece of data which are major is selected as the final result.*

Example 2 *Assume that, in cooperative intrusion detections, four cooperators believe that the host with IP 192.168.150.77 are suffering from the PHPKIT remotely inject SQL script attack, and one cooperator believes that the host is*

Log 1: Aug 24 2017 08:54:48: %ASA-4-106023: Deny tcp src outside:192.168.208.63/46857 dst inside:192.168.150.77/443 by access-group "OUTSIDE" [0x5063b82f, 0x0]
Log 2: Jan 13 2014 13:46:36: %ASA-4-106023: Allow tcp src outside:192.168.208.63/46857 dst inside:192.168.150.77/443 by access-group "OUTSIDE" [0x3028fa8e, 0x2]

Figure 2: Time-priority-based combination

suffering from the PYTHONKIT remotely inject SQL script attack. According to the majority-priority policy, the final combination result is PHPKIT remotely inject SQL script.

Policy 3 *(Low risk priority): If more than one data sources should be combined into one piece of data, the combination with the lowest risk is adopted.*

Access control [Yu et al., 2018, Yu et al., 2017] is important to ensure data security. Next, we give the declassification and endorsement in access control models as an example to show the low-risk policy.

In access control, Bell-LaPadula model and Biba model [Matt, 2003] are often used to provide confidentiality and integrity, respectively. In the basic Bell-LaPadula model, the confidentiality levels with partial order relationship(e.g., public$\leq$ confidentiality$\leq$ secret$\leq$ top secret) are designed to label data and accessors. Only if the level of an accessor is greater than or equal to the level of the accessed data, the accessor can read the data; Only if the level of an accessor is less than or equal to the level of the accessed data, the accessor can write the data.

In the basic Biba model, an integrity level with partial order relationship (e.g., low integrity $\leq$ middle integrity $\leq$ high integrity) is used to label data and accessors. Only if the integrity level of an accessor is greater than or equal to the integrity level of the accessed data, the accessor can write the data; Only if the integrity level of an accessor is less than or equal to the integrity level of the accessed data, the accessor can read the data.

We use $C = \{public, confidentiality, secret, topsecret\}$ to denote a set of confidentiality levels and $I = \{low\text{integrity}, \text{middleintegrity}, \text{highintegrity}\}$ to denote a set of integrity levels. For simplicity, tuple (c, i) is used to denote a security level, where $c \in C$ and $i \in I$. Given two security levels (c_1, i_1) and (c_2, i_2), formula $(c_1, i_1) \leq (c_2, i_2)$ holds, if both $c_1 \leq c_2$ and $i_2 \leq i_1$ hold. We use $risk(d_x : (c_x, i_x), d_y : (c_y, i_y), d_z : (c_z, c_z))$ to denote the risk when combining d_x with security level (c_x, i_x) and d_y with security level (c_y, i_y) into d_z with security level (c_z, i_z). Next, we discuss combination between d_1 with security level (c_1, i_1) and d_2 with security level (c_2, i_2) in different access scenes (the obtained data through combination are $d_3 : (c_3, i_3)$).

Scene 1. Assume that $(c_1, i_1) \leq (c_2, i_2)$, the security level of all accessors are higher than (c_2, i_2), and only operation of all accessors to data d_3 is *read*. In this scene, according to Bell-LaPadula model and Biba model, all accessors can read d_3 no matter whether the level of data d_3 is (c_1, i_1) or (c_2, i_2). Because of $(c_1, i_1) \leq (c_2, i_2)$, the risk brought by data $d_3 : (c_2, i_2)$ is less than by data $d_3 : (c_1, i_1)$ (i.e., $risk(d_1 : (c_1, i_1), d_2 : (c_2, i_2), d_3 : (c_1, c_1)) \leq risk(d_1 : (c_1, i_1), d_2 : (c_2, i_2), d_3 : (c_2, c_2))$). According to Policy 3, the obtained data is d_3 with security level (c_2, i_2).

Scene 2. Assume that $(c_1, i_1) \leq (c_2, i_2)$, the security level of all accessors equals (c_1, i_1), and only operation of all accessors to data d_3 is *read*. In this scene, all accessor can read d_3 only if the level of data d_3 is (c_1, i_1). If the security level of d_3 is labeled as (c_1, i_1), then the risk of data leakage might exit (because the confidentiality level in d_3 is c_2 ($c_2 \geq c_1$)). However, if security level of d_3 is labeled as (c_2, i_2), then the availability risk might exit (because the accessors with security level (c_1, i_1) can not read d_3. According to Policy 3, if formula $risk(d_1 : (c_1, i_1), d_2 : (c_2, i_2), d_3 : (c_1, c_1)) \leq risk(d_1 : (c_1, i_1), d_2 : (c_2, i_2), d_3 : (c_2, c_2)))$ holds, then the security level of d_3 is (c_1, i_1); otherwise, its level is (c_2, i_2).

4 Conclusions

To provide security for network and information systems, it is necessary to measure security. Due to massiveness and heterogeneity of data from different sources, it is difficult to classify and combine data on demand. In this paper, considering implication relationship of metrics, we propose a combination model and combination policy for security measurement.

Acknowledgements

This work is supported by the National Key Research and Development Program of China (No.2016YFB0800704), the National Natural Science Foundation of China (No. 61672515), and Strategic Priority Research Program of Chinese Academy of Sciences (No.XDC02040400).

References

[Angelov and Yager, 2013] Angelov, P. and Yager, R. "Density-based averaging-A new operator for data fusion". Information Sciences, 222: 163-174.

[Charte et al., 2018] Charte, D., Charte, F., García, S., del Jesus, M. J., and Herrera, F. "A practical tutorial on autoencoders for nonlinear feature fusion: Taxonomy, models, software and guidelines". Information Fusion, 44: 78-96.

[Chen and Varshney, 2002] Chen, B. and Varshney, P. K. "A Bayesian sampling approach to decision fusion using hierarchical models". IEEE Transactions on Signal Processing, 50(8): 1809-1818.

[Chen et al., 2016] Chen, Y., Jiang, H., Li, C., Jia, X., and Ghamisi, P. "Deep feature extraction and classification of hyperspectral images based on convolutional neural networks". IEEE Transactions on Geoscience and Remote Sensing, 54(10): 6232-6251.

[Dong et al., 2014] Dong, Z., Zheng, C., and Zhang, G. "Self-adaption of Weighted Average Research for Data Fusion with Different Precision". Ship Electronic Engineering, 34(10): 31–33.

[Du et al., 2015] Du, Y., Wang, W., and Wang, L. "Hierarchical recurrent neural network for skeleton based action recognition". in Proceedings of the IEEE conference on computer vision and pattern recognition, pages: 1110-1118.

[Fan et al., 2014] Fan, Y., Sherman, R., and Shum, M. "Identifying treatment effects under data combination". Econometrica, 82(2): 811-822.

[Fatemipour et al., 2014] Fatemipour, F., Akbarzadeh-Totonchi, M. R., and Ghasempour, R. "A new fuzzy approach for multi-source decision fusion". in Proceedings of the IEEE International Conference on Fuzzy Systems, pages: 2238-2243.

[Fontani et al., 2013] Bianchi, M. T.,De Rosa, A., Piva, A., and Barni, M. "A framework for decision fusion in image forensics based on Dempster-Shafer Theory of Evidence". IEEE Transactions on Information Forensics and Security.

[Ghosh, 2017] Ghosh, S. "Cross-domain data fusion for disaster detection". Doctoral dissertation.

[Graham et al., 2016] Graham, B. S., Pinto, C. C. d. X., and Egel, D. "Efficient estimation of data combination models by the method of auxiliary-to-study tilting (ast)". Journal of Business Economic Statistics, 34(2): 288-301.

[Hall and Llinas, 1997] Hall, D. L. and Llinas, J. "An introduction to multisensor data fusion". Proceedings of the IEEE, 85(1): 6-23.

[Jang et al., 2017] Jang, H., Plis, S. M., Calhoun V. D., and Lee, J. H. "Task-specific feature extraction and classification of fmri volumes using a deep neural network initialized with a deep belief network: Evaluation using sensorimotor tasks". NeuroImage, 145: 314-328.

[Khaleghi et al., 2013] Khaleghi, B., Khamis, A., Karray, F. O., and Razavi, S. N. "Multisensor data fusion: A review of the state-of-the-art". Information Fusion, 14(1): 28-44.

[Komarova et al., 2018] Komarova, T., Nekipelov D., and Yakovlev, E. "Identification, data combination, and the risk of disclosure". Quantitative Economics, 9(1): 395-440.

[Kuncheva et al., 2001] Kuncheva, L. I., Bezdek, J. C., and Duin, R. P. "Decision templates for multiple classifier fusion: an experimental comparison". Pattern Recognition, 34(2): 299-314.

[Li et al., 2019] Li, Y., Yu, Y., Susilo, W., Min, G., Ni, J., and Choo, R. "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems". IEEE Transactions on Dependable and Secure Computing, 16(1): 72-83.

[Matt, 2003] Matt, B. "Computer security: art and science". Addison-Wesley Professional.

[Nguyen et al., 2018] Nguyen, D., Nguyen, K., Sridharan, S., Dean, D., and Fookes, C. "Deep spatio-temporal feature fusion with compact bilinear pooling for multimodal emotion recognition". Computer Vision and Image Understanding, 174: 33-42.

[Ribeiro et al., 2014] Ribeiro, R. A., Falcão, A., Mora, A., and Fonseca, J. M. "FIF: A fuzzy information fusion algorithm based on multi-criteria decision making". Knowledge-Based Systems, 58: 23-32.

[Romero et al., 2016] Romero, A., Gatta C., and Camps-Valls, G. "Unsupervised deep feature extraction for remote sensing image classification". IEEE Transactions on Geoscience and Remote Sensing, 54(3): 1349-1362.

[Shao et al., 2017] Shao, H., Jiang, H., Wang, F., and Zhao, H. "An enhancement deep feature fusion method for rotating machinery fault diagnosis". Knowledge-Based Systems, 119: 200-220.

[Wang et al., 2014] Wang, Z., Zhang, D., Zhou, X., Yang, D., Yu, Z., and Yu, Z. "Discovering and profiling overlapping communities in location-based social networks". IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44(4): 499-509.

[Xing et al., 2016] Xing, C., Ma, L., and Yang, X. "Stacked denoise autoencoder based feature extraction and classification for hyperspectral images". Journal of Sensors, 2016, 2016.

[Xue et al., 2019] Xue, L., Yu, Y., Li, Y., Au, M. H., Du, X., and Yang, B. "Efficient attribute-based encryption with attribute revocation for assured data deletion". Information Science, 479: 640-650.

[Yu et al., 2017] Yu, Y., Au, M. H., Ateniese G., Huang, X., Susilo, W., Dai, Y., and Min, G. "Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage". IEEE Transactions on Information Forensics and Security, 12(4): 767-778.

[Yu et al., 2018] Yu, Y., Li, Y., Du, X., Chen, R., and Yang, G. "Content Protection in Named Data Networking: Challenges and Potential Solutions". IEEE Communications Magazine, 56(11): 82-87.

[Yu et al., 2017] Yu, Y., Li, Y., Yang, B., Susilo, W., Yang G., and Bai, J. "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage". IEEE Transactions on Emerging Topics in Computing. Online.

[Yu et al., 2018] Yu, Y., Xue, L., Li, Y., Du, X., Guizani, M., and Yang, B. "Assured Data Deletion with Fine-Grained Access Control for Fog-Based Industrial Applications". IEEE Transactions on Industrial Informatics, 14(10): 4538-4547.

[Zhang and Ge, 2015] Zhang, F. and Ge, Z. "Decision fusion systems for fault detection and identification in industrial processes". Journal of Process Control, 31: 45-54.

[Zheng, 2015] Zheng, Y. "Methodologies for cross-domain data fusion: An overview". IEEE Transactions on Big Data, 1(1): 16-34.