Journal of Computer Science 8 (4): 564-572, 2012
ISSN 1549-3636

Purpose-based Versus Flow-based Access Control for Privacy

Sabah Al-Fedaghi, Bashayer Al-Babtain and Maha Al-Fahad
Department of Computer Engineering, College of Engineering and Petroleum
Kuwait University, 5969, Safat 13060, Kuwait

Abstract: Problem statement: Data protection legislation requires handling of Personal Identifiable Information (PII) in special ways to guarantee privacy. Specifically, the notion of handling purpose plays an important role in current access control mechanisms that allow only actions corresponding to intended purposes. A problem that arises in this context is how to ensure that PII is used solely for the intended purpose. **Approach:** This study shows that problems in the context of purpose access control can be avoided by using flow-based specifications that map users to a sequence of stages of flows of PII. The methodology is used as a tracking apparatus as it specifies the types of operations a user can perform on such information. The flow system of PII is constructed from six generic operations. **Results:** The resultant maps of flows of PII are used to assign flow systems to users that represent access control instruments to specify permissible operations and PII streams, preventing use of PII for purposes not corresponding to intended purposes. **Conclusion:** The resultant flow-based access map demonstrates a viable description method that can be adopted for controlling access to PII. It also presents a uniform methodology that can be applied at various levels such as privacy policies.

Key words: Conceptual modeling, purpose control, PII handling, information flow, privacy policies, information technology, privacy protection, information systems, access control

INTRODUCTION

Advances in information technology and the emergence of privacy-invasive technologies have made it necessary to introduce privacy regulations that impose restrictions on handling of Personal Identifiable Information (PII). According to current thinking, "PII privacy protection can only be achieved by enforcing privacy policies within an organization's online and offline data processing systems" (He and Anton, 2003) and "privacy cannot be efficiently implemented solely by legislative means. Data protection commissioners are therefore demanding that legal privacy requirements should be technically enforced and should be a design criteria for information systems" (Fischer-Hubner and Ott, 1998).

This means that privacy requirements should be incorporated into automated methods of handling PII. Handling of PII (input, output, processing) leads to development of access control mechanisms for this type of information. Access control is a means for restricting access (e.g., who, what, what type) to resources (e.g., files or data, programs, devices) and functionality provided by computer applications. This restriction may involve time, type of request (e.g., access to a certain IP address), type of encryption client can support and so forth. Authentication, authorization and audit are types of access control. Classical access control is basically the process of deciding whether a user has a permission to perform an operation such as reading, writing, executing, deleting, or searching for an object. A model in this context shows the organization of permissions of users. Many types of access control methodologies exist, including Discretionary Access Control, Mandatory Access Control and Role-based Access Control (RBAC).

The notion of purpose plays a central role in the legislative aspects of PII privacy. Purpose (possibly multiple) associated with a given PII specifies its intended handling. Technically, this means incorporating the purpose of handling PII into the access control mechanism of the information system. According to Byun and Li (2008):

> The notion of purpose must play a major role in access control models and ... an appropriate metadata model must be developed to support such privacy centric access control models… A privacy policy mainly concerns with which data object is used for which purpose (sec). Consequently, purpose is a central concept in many privacy protecting access control models".

Corresponding Author: Sabah Al-Fedaghi, Department of Computer Engineering, Kuwait University, 5969, Safat 13060, Kuwait

In this study, we do not hastily import the notion of purpose from privacy legislation and guidelines; rather, we suggest that instead of such a verbose and conceptually difficult concept, access control to PII ought to be based on the sequence of flows of operations performed on PII. This idea was originally presented by Al-Fedaghi (2007e).

Motivational example: Petkovic *et al*. (2011) consider a hospital system (HIS) where patient PII is stored in records (EPR). HIS controls access to EPR according to purposes. Suppose that a patient, Jane, did not give the hospital consent to process her PII for research purposes:

> If the patient is referred to a cardiologist, the cardiologist accesses patient medical history in HIS and makes a medical examination to collect the symptoms (T06). Based on this information, the cardiologist can either make a diagnosis directly (T07), or request lab tests or radiology scans (T08 and T09, respectively). If the resulting tests and scans are not good or a diagnosis cannot be made based on them, further tests can be required.

Figure 1 shows a partial view of a diagram used in this example, specified in Business Process Modeling Notation (BPMN) Object Management Group, 2009.

The problem is addressed by Petkovic *et al*. (2011) as follows:

> The cardiologist can get access to patient information for the legitimate purpose (i.e., claiming that it is for healthcare treatment) and then use the data for research purposes.

Preventive mechanisms are not able to cope with these situations. In particular, they cannot prevent a user from processing data for other purposes after the same user has legitimately gained access to them (Petkovic *et al*., 2011).

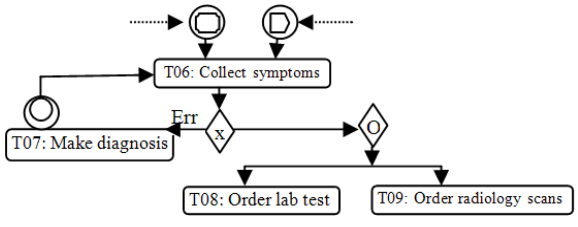

Fig. 1: Cardiologist health treatment process (partial figure from Petkovic *et al*., 2011)

They propose the following solution:

> An approach that enables purpose control by determining if an audit trail is a valid execution of the process used by the organization to implement the intended purposes... This implies verifying that every usage of patient information is part of the sequence of tasks that the cardiologist and the other parties involved in the provision of healthcare treatments have to perform in order to accomplish the goal.

This problem is taken as a sample of problems that occur in current methodologies of incorporating PII protection into information systems. The approach presented in this study solves such a problem in particular and also introduces diagrammatic specifications as an alternative to current representations that incorporate privacy requirements into purpose-based access control mechanisms.

Since current purpose-based access control methodologies are applied in the context of RBAC, the next section briefly describes such a model while concentrating on the notion of role.

Access control: "Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system" (Vincent *et al*., 2006). The objectives of an access control system are often described in terms of protecting system resources against inappropriate or undesired user access. An information system can implement access control systems at different levels. Operating systems employ access control to protect files and directories. Database management systems apply access control to regulate access to data. Application systems may implement access control independent of the operating systems and/or database systems on which they are installed.

RBAC (Ferraiolo *et al*., 2007) is a multilevel security mechanism that associates roles with individual users in order to determine their access rights. In the RBAC framework, users are given roles based on their position in a particular organization. RBAC is used according to the organization's role ontology, e.g., organizational hierarchy. The essence of role-based access control lies in the notion of role as an intermediary between subjects (e.g., users) and objects (e.g., resource): roles are given access rights to objects while subjects are associated with roles.

To determine the "purpose" of access, Byun and Li (2008) rely on RBAC models; nevertheless, they also declare that "the concept of purpose has not yet been thoroughly investigated" and "formally" define it as "the reason(s) for data collection and data access".

Intended purpose refers "to purposes associated with data and thus regulating data accesses". According to Tschantz *et al*. (2011), "Byun and Li (2008) … associate purposes with sensitive resources and with roles and their method only grants the user access to the resource when the purpose of the user's role matches the resource's purpose. The method does not, however, explain how to determine which purposes to associate with which roles".

Since there are several definitions of PII, we next introduce the definition of PII adopted in this study.

MATERIALS AND METHODS

Systems of personal identifiable information: (Summarized/ copied from Al-Fedaghi (2005; 2006a-d; 2007a-d; 2011) for the sake of a self-contained paper) the concept of PII assumes two basic types of entities: natural persons and non-natural persons. PII is any information for which the referent signifies a natural person. The referent is said to be the proprietor of PII.

The formal semantics of the word referent are very important in this line of thought. The "referent" is recognized by mapping the word (logical name) in relation to the actual object (natural person) in reality. This mapping to a natural person limits possible extension to specific human beings. PII is any information that is a referent to uniquely identifiable persons. Every PII refers to its proprietor(s) in the sense that it "leads to" him/her/them as distinguishable entities in the world.

Accordingly, there are two types of PII:

- Atomic PII (APII), where the expression refers to a single proprietor
- Compound PII (CPII), where the expression refers to more than one proprietor

PII flow model (denoted FM): Information including PII is a type of "thing that flows" or flowthing. Flowthings are things that are created, released and transferred, arrive, are accepted and are processed (each is called a stage of a PII lifecycle) according to a flow system (flowsystem), as shown in Fig. 2. The environment of the flowsystem is called its *sphere* (e.g., department, pharmacy). The notions of flowthings and flowsystems have been used in many applications.

Consider a situation where PII "enters" (e.g., from a patient) the sphere of a hospital. PII flows to the *transfer* stage (input/output ports or component) of the hospital. When PII is completely in the location of the hospital (e.g., in the buffer of its information system), it has *arrived*. Arrival does not guarantee acceptance since opening of a patient record may be cancelled, e.g., because of incomplete documents. If PII is *accepted*, then it may be *processed* (e.g., tabulated, reformulated, translated, summarized). New PII may be *created*, e.g., a physician's diagnosis. The hospital may *release* PII to others. PII may stay in the released stage for awhile because the channel of communication is temporarily down. These six stages in the life cycle of any flowthing are exclusive (e.g., PII cannot be in two stages simultaneously). More details of this model are given in the references mentioned above. For the purpose of simplification, the stage of Received will be used instead of Arrive and Accept whenever every flowthing that arrives is accepted.

Example: Consider a general FM representation of the cardiologist health treatment process shown in Fig. 3. For the sake of simplicity, we consider two spheres: that of the Cardiologist and that of the Laboratory (shown in detail in Fig. 4). The Cardiologist's sphere has four flowsystems: Patient record, Request (for lab), Lab report and Diagnosis. The Lab's sphere also includes four flowsystems: Request, Test, scan and report. The solid arrows indicate a flow and the dashed arrows represent triggering. Circles are used to label the steps described in the text.

In Fig. 4, a patient record flows to the cardiologist (e.g., from a hospital), where it is transferred (circle 1-e.g., connection to a network), received (e.g., e-mail) and processed. This processing triggers (circle 2) creation (circle 3) of a request for tests and scanning that flows to the laboratory (circle 4).

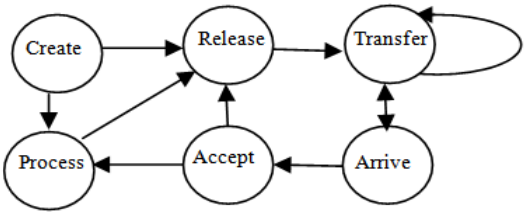

Fig. 2: Flowsystem, assuming that no released flowthing is returned

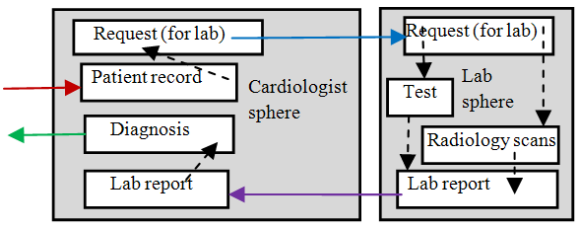

Fig. 3: Brief FM description of flows in the example

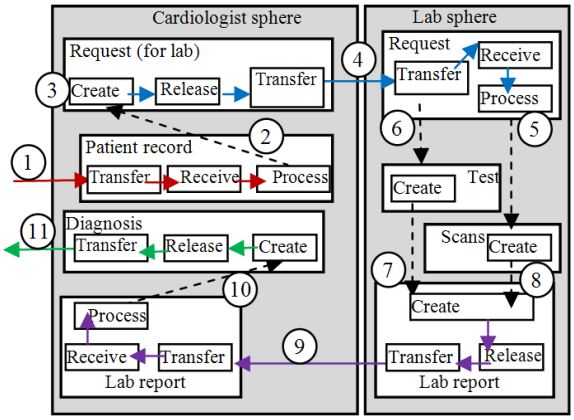

Fig. 4: Detailed FM description of flows in the example

In the laboratory, the received request is processed, triggering scans (circle 5) and tests (circle 6). The tests and scanning trigger (circles 7 and 8) a lab report that flows (circle 9) to the cardiologist. The cardiologist processes the report, which triggers (circle 10) creation of his/her diagnosis, which flows to the hospital (circle 11).

This FM description gives the backbone of basic involved flows and operations that can be superimposed with other details such as synchronization, logical con-disjunctions, constraints, rules. It is like a map of a city that includes streets, buildings, lots and factories, supplemented with representations of things that flow in and among these components and basic operations that are performed on these things. Notice that storage, dumping grounds, copying, waste disposal,…can be added to the FM six-stage model, but such operations are secondary since they can occur in any of the stages.

RESULTS

General model for PII handling: Consider basic entities involved in handling of PII of a proprietor. First there is the non-proprietor that handles PII taken directly from its proprietor. A non-proprietor can collect PII from another non-proprietor, e.g., a company that buys PII from another company. Figure 5 shows a general picture of a PII environment involving a proprietor along with direct and indirect brokers.

Purpose-based access: The notion of purpose appears in all privacy guidelines, codes, policies and legislation. It plays a central role in many privacy-related systems such as P3P, Hippocratic databases, EPAL, XACML and many applications, e.g., (Kuang *et al*., 2011; Hu *et al*., 2006). For example, the Data Quality Principle in the OECD guidelines specifies:

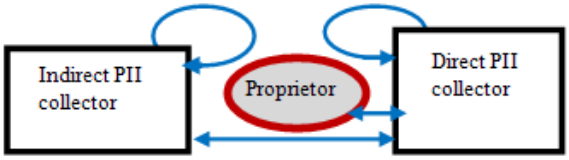

Fig. 5: Basic entities involved in handling of PII

> Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. (OECD, 1980)

According to the World Wide Web Consortium, 2007:

> A purpose specifies the intended use of the data element" and it "describes the reason(s) for data collection and data access" (Byun and Li, 2008). P3P specifies such purposes as: administration, development, contact, telemarketing.

Purpose as it is used in such contexts is not limited to "purpose of access" as it is used in purpose-based access control. It is possible to collect, use, transfer, receive, ... PII without accessing it (e.g., because of encryption). For example, collecting PII without access is analogous to money transfer guards who collect boxes of money without laying an eye on the money. It is also possible to access PII without a purpose in the sense of guidelines. It is possible that PII within the information system is accessed, for no purpose other than to retrieve another PII record. Consequently, in practice the purpose may be specified without proprietor involvement in the system.

The "purpose of privacy guidelines" is different from the "purpose of access control" and can be vague and overly verbose. Tschantz *et al*. (2011) give an interesting example of such ambiguity:

> Consider a physician working at a hospital who, as a specialist, also owns a private practice that tests for bone damage using a novel technique for extracting information from X-ray images. After seeing a patient and taking an X-ray, the physician forwards the patient's medical record including the X-ray to his private practice to apply this new technology… The physician claims that this consultation was for reaching a diagnosis. As such, it is for the purpose of treatment and, therefore, allowed under each of these policies.

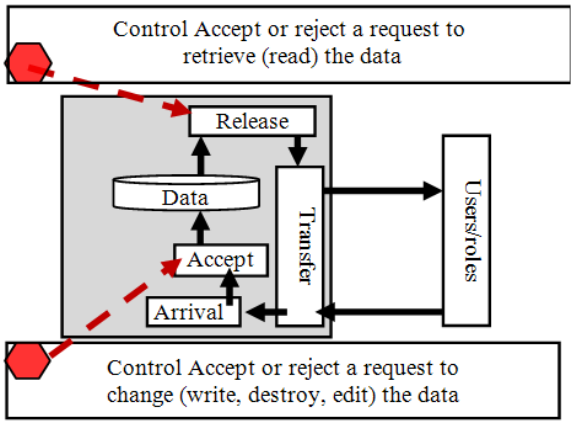

Fig. 6: Conceptualization of basic "access control"

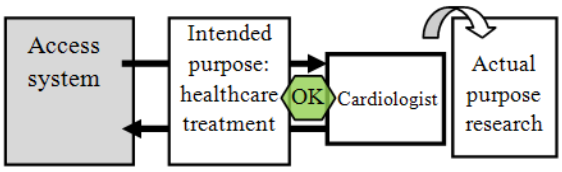

Fig. 7: The cardiologist can access patient information for a legitimate purpose and then use the data for research purposes

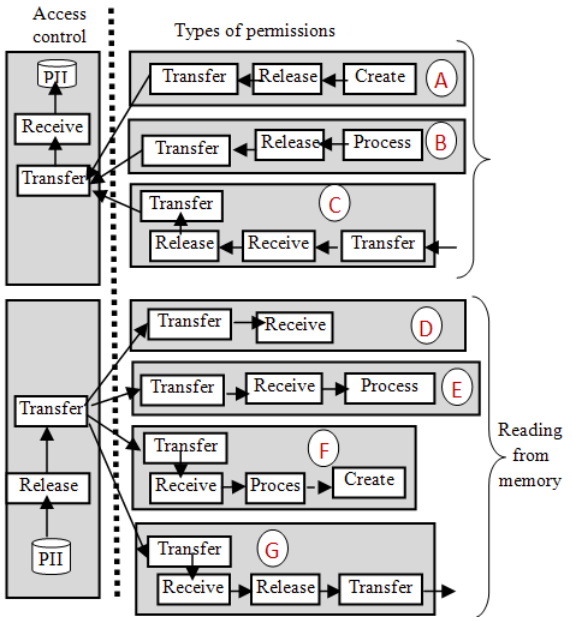

Fig. 8: Set of basic permissions of accessing PII

In general, purposes stated as reasons are given in response to *why* questions. Why is PII collected? The answer: it is used in "telemarketing", "delivery". Such a reason is not satisfactory even if supplemented by a descriptive sentence. This is analogous to agreeing to give money (at times PII is worth more than that) to someone because the person claims vaguely that the money is "to be used for trading". Obviously, a person would need a far more detailed reason to agree to the proposal. In the P3P purpose of Individual Decision, "Information may be used to determine the habits, interests, or other characteristics of individuals and combine it with identified data to make a decision that directly affects that individual" P3P, 2006. This sounds like a better description because it answers not only the reason (why?) for collecting information, but also *how* to reach a decision.

The "purpose of the privacy guidelines" is mainly to inform proprietors. Imagine a data collector telling a patient from whom PII is gathered the different purposes for which his/her PII will be put to use, including P3P's purpose of "Completion and Support of Activity For Which Data Was Provided". Or, declaring when gathering PII from a proprietor that one of the reasons, relevant (OECD guidelines) to his/her data, is "maintenance of our computer system," a purely technical matter that does not make sense to the proprietor who is worrying about his/her PII.

On the other hand, "access control purpose" is directed at users of PII. It is a permission system that provides methods to allow a user to create, update, destroy, view and edit a record. To emphasize the context of access control, Fig. 6 shows a conceptualization of a basic access control mechanism.

The purpose-based access control mechanism replaces roles with purposes. To contrast the difference against a pure access control system, we can conceptualize the Cardiologist Health Treatment Process given by Petkovic *et al*. (2011), as shown in Fig. 7. The cardiologist can access patient information for a legitimate purpose (i.e., claim that it is for healthcare treatment) and then use the data for research purposes. As seen in the figure, the system has no control of PII after it releases it.

Controlling access to PII may not coincide with rules (e.g., legislation) for collecting and/or handling of PII. In fact, roles in RBAC can be conceptualized as purposes: that of a researcher is "to conduct research", of an administrator "to manage transactions", of a "student "to register in courses". Access purpose can be a role, e.g., "to provide healthcare treatment" becomes "health provider", "completion and support of activity for which data were provided" becomes "system supervisor".

FM-based permissions: An alternative method for access control of PII is use of FM to identify generic operations and assign users/roles in these operations. The model provides the basic permissions to the user shown in Fig. 8:

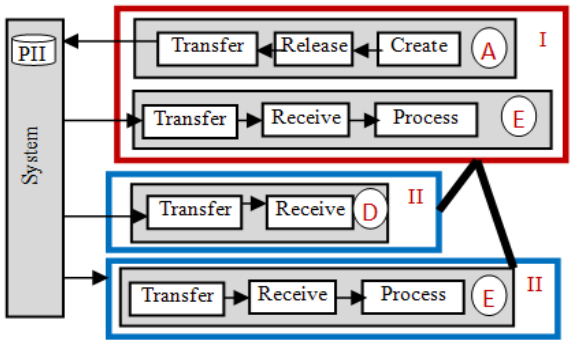

Fig. 9: User I can read/write PII, user II can only access it (e.g., only review it on screen), while user III can access it and process it

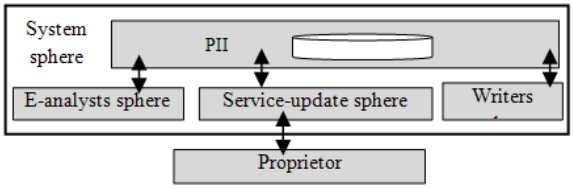

Fig. 10: All types of access to PII are controlled by the system

- Permission to store PII generated by the user
- Permission to store PII processed by the user
- Permission to write PII received by the user
- Permission to access (receive) PII
- Permission to process (e.g., tabulate) PII
- Permission to process PII to create new PII (e.g., data mining)
- Permission to transfer PII, e.g., to printer, e-mail

All types of relationships (e.g., hierarchies) can be applied to this method of access control. For example, in Fig. 9, User I can create, receive and process PII; his subordinate II can only read it (watch it on screen) and process it (summarize, compress).

DISCUSSION

Example: This example is a revised version of the example given by Byun and Li (2008). Suppose that we wish to allow three types of users:

E-Analysts are users who analyze customer PII and prepare the contents of e-mails. They have the necessary permissions to access customer profiles.

Writers are users who write and send out e-mails to customers. They have permissions to access customers' e-mail addresses.

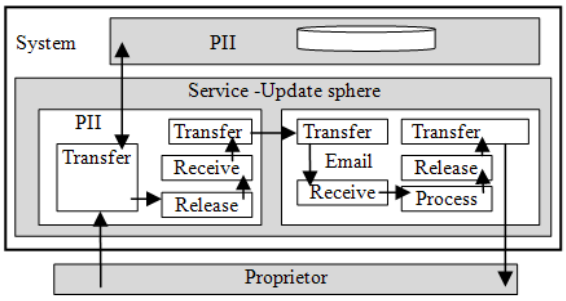

Fig. 11: Service-Update streams of PII flow

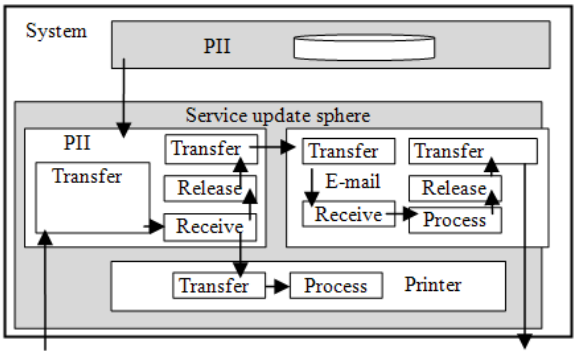

Fig. 12: Service-Update streams of PII flow with permission to print PII

Service-Update refers to workers who send out updated service information and then update the information in the system.

In this scenario, we have three agents, the proprietor and the system as an agent. The *system* represents the total information system of which the three agents are users. The system provides viewing of (access to) PII to other agents, as shown in Fig. 10. The structure of the FM description provides a means for monitoring access control by the system. Permissions can be declared at any point in the PII flow. Figure 11 shows the details of flow of PII to Service-Update.

According to Tschantz *et al*. (2011), in role-based access control, "A user in a role can perform actions that do not fit the purposes associated with his role, allowing him to use the resource for a purpose other than the intended one". No such problem arises when FM methodology is used. The Service-Update agent is limited to releasing PII, transferring it to e-mail and releasing the e-mail. Note that the Service-Update agent cannot store, print, or receive PII. If we wish to allow the Service-Update agent to print PII, then we must assign the flows shown in Fig. 12.

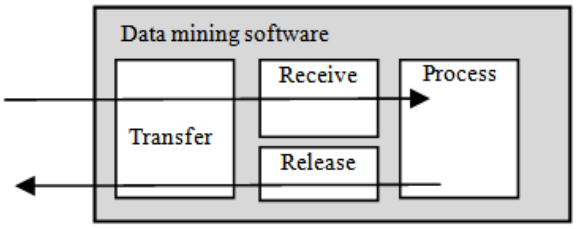

Fig. 13: Service-Update streams of PII flow with permission to print PII

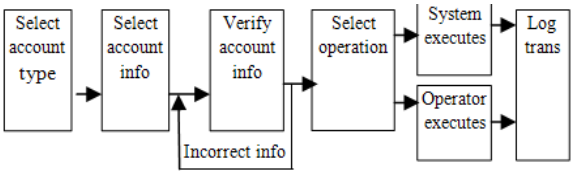

Fig. 14: Banking Workflow model (partially from Alhaqbani *et al*., 2009)

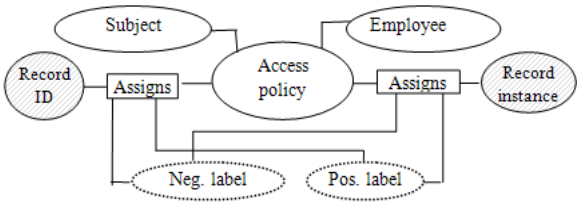

Fig. 15: Conceptual model: authorization (partially from Alhaqbani *et al*., 2009)

Suppose that the Service-Update agent decides to use incoming PII in another application, such as data-mining software (e.g., for research purposes). Simply, the agent can do this only if the flow system shown in Fig. 13 is in the agent's PII sphere. Any application software is a sphere by itself.

Also, the problem addressed by Petkovic *et al*. (2011) and discussed previously does not arise in FM flow-based access control. A cardiologist can access patient PII for a legitimate purpose (e.g., claiming it is for healthcare treatment), but he cannot use the data for research purposes (e.g., a clinical trial). The cardiologist is prevented from using any research tools with PII because he/she cannot direct the flow of PII to such application. The flow-based description, by itself, can be specified such that he/she cannot download the PII or even print it.

Proprietor role in access control: Alhaqbani *et al*. (2009) used an example from the banking sector to illustrate a workflow model, shown in Fig. 14 (also Alhaqbani, 2010). The banking workflow model receives and processes customer requests and queries. The bank operator interacts with the system through a series of pages. The operator begins by selecting a certain customer account using the account information. The selected account information is then displayed for the operator. Once the operator verifies the account information, a selected operation is performed on that particular account. After processing the operation, the system logs the transaction details.

In this particular case, the customer has no power to limit the PII of his/her bank account seen by the bank's operator, because data access control implements the bank's security policy with no consideration of the customer's privacy. For example, a customer might desire to hide his/her credit card balance from the bank operator; this customer's privacy policy is currently not implemented in the mentioned workflow.

The workflow methodology used (Fig. 14) mixes the flow of customer PII and system-related flows. Some arrows in Fig. 14 represent the customer's PII while others represent loading of different pages to the operator. Separating the flows as in the FM gives a more systematic view for applying privacy policies.

The solution offered by Alhaqbani *et al*. (2009) is a conceptual OR model designed to enforce user privacy policies in workflow systems. Figure 15 shows a partial view of this solution. Each access policy has a unique ID and must be set by a proprietor of PII to authorize or restrict the capabilities of employees. Positive and negative authorization approaches are used to express privacy requirements. Positive labels are assigned to allow access and negative labels are assigned to deny access to data. The model discusses some implementation details such as negative and positive labels and record ID and record instance.

The FM framework can provide a conceptual model for authorization in such a system while giving the implementer flexibility in choosing implementation details. The FM model corresponding to the example is shown in Fig. 16. The system includes two spheres: one for the employee and one for proprietor (customer). Each can view and handle the flowsystem in its sphere; however, other non-account PII (e.g., a credit card) is within the proprietor's sphere. If the employee desires access to this information, the employee creates a request (circle 1) that flows to the customers' requests flowsystem (circle 2), where it is processed and according to the customer's access policy, the request is either accepted or rejected.

After the information is accepted, it is processed, triggering the creation of a certain request. The request (for an operation) flows to the subject's sphere inside the

system (circle 2). The received request is processed in the proprietor's sphere (circle 3), where the authorization is really enforced. The process includes checking the proprietor's privacy policies and comparing with the received request from the employee.

This example brings up an interesting angle in privacy research that is raised in this field of study: the notion of perceived privacy (Adams, 1999; 2001). According to Adams (1999), "the main problem is that current approaches to privacy define characteristics of the data and thus information, rather than how it is perceived by the users". Janse *et al*. (2007a) define perceived privacy as "the perceived control a user has over how, when and to what extent information about oneself is released to another person or system within a social context" According to Janse *et al*. (2007b):

> "Perceived privacy" or how end-users perceive that the system affects their privacy, is one of the key aspects for the acceptance of ambient intelligent systems by users. It is also one of the most complex problems to handle. It is about 'how, when and to what extent' data about people are revealed to other people within a dynamic social context.

This indicates that the proprietor expects the PII custodian (e.g., the bank) to have a similar attitude regarding:

- Appreciation of sensitivity of PII
- Mutual trust between them
- Careful handling (usage) of PII

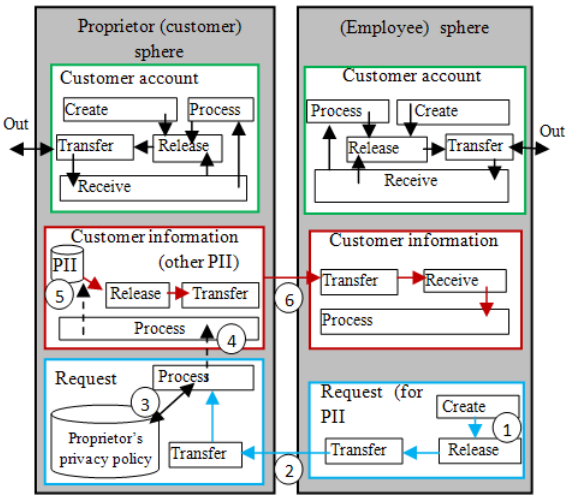

Fig. 16: FM-based description of access authorization

In the FM approach, as demonstrated in this example, the proprietor participates in handling his/her PII through accessing his/her PII flowsystem and setting access policy, even with respect to employees of the bank.

CONCLUSION

Information security, protection and privacy of data are critically important in any system development. Privacy requirements are carefully considered when developing information systems. Data protection legislation requires handling Personal Identifiable Information (PII) in special ways. Specifically, the notion of purpose has played an important role in current mechanisms that allow only actions corresponding to intended purposes. This study provides a solution for such a purpose control problem by using flow-based specifications that map users to the sequence of stages of flow assigned to the user. The methodology depicts flows of PII and uses it as a tracking apparatus for specification of the types of operations a user can perform on such information. The flow system of PII is constructed from six generic operations of "handle" descriptions.

The introduced methodology presents an alternative way of specifying access control in purpose-based methods. It also provides a uniform method for policy specification. Further research should explore the possibility of applying FM descriptions in different areas such as networks and dynamic environments.

REFERENCES

Adams, A., 1999. The implications of users' multimedia privacy perceptions on communication and information privacy policies. Proceedings of the Telecommunications Policy Research Conference, (TPRC' 99), Washington, DC., pp: 1-20.

Adams, A., 2001. Users' perceptions of privacy in multimedia communications. PhD thesis, school of psychology, University College London.

Al-Fedaghi, S.S, 2005. How to calculate the information privacy. Proceedings of the 3rd Annual Conference on Privacy, Security and Trust, Oct. 12-14, St. Andrews, NB, Canada, pp: 3-13.

Al-Fedaghi, S.S, 2006a. Anatomy of personal information processing: Application to the EU privacy directive. Int. J. Liability Sci. Enquiry, 1: 129-138. DOI: 10.1504/IJLSE.2007.014586

Al-Fedaghi, S.S, 2006b. Personal management of private information. Proceedings of the IEEE International Conference on Innovations in Information Technology (IIT2004), Nov. 19-21, Dubai, pp: 1-5. DOI: 10.1109/INNOVATIONS.2006.301955

Al-Fedaghi, S.S, 2006c. Personal information flow model for P3P. Proceedings of the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Ispra, Italy, pp: 17-18.

Al-Fedaghi, S.S, 2006d. Aspects of personal information theory. Proceedings of the 7th Annual IEEE Information Assurance Workshop, Jun. 21-23, IEEE Xplore Press, West Point, New York, pp: 155-162. DOI: 10.1109/IAW.2006.1652090

Al-Fedaghi, S., 2007a. Dismantling the twelve privacy purposes. Proceedings of the IFIP Joint iTrust and PST Conferences on Privacy, Trust Management and Security, Jul. 30-Aug. Springer.

Al-Fedaghi, S., 2007b. When reinventing principles is necessary. Proceedings of the 7th International Computer Ethics Conference, (ICEC' 07), University of San Diego, USA., pp: 12-14.

Al-Fedaghi, S.S., 2007c. Incorporating personal information into RDF. Proceedings of the IRMA International Conference, (IRMAIC' 07), Idea Group Inc., Vancouver, Canada, pp: 119-122.

Al-Fedaghi, S., 2007d. How sensitive is your personal information? Proceedings of the 2007 ACM Symposium on Applied Computing, Mar. 11-15, ACM, Seoul, Korea, pp: 165-169. DOI: 10.1145/1244002.1244046

Al-Fedaghi, S., 2007e. Beyond purpose-based privacy access control. Proceedings of the 18th Conference on Australasian Database, (CAD' 07), ACM, New York, pp: 23-32.

Al-Fedaghi, S., 2011. Toward a unifying view of personal identifiable information. Proceedings of the 4th International Conference on Computers, (ICC' 11), Privacy and Data Protection, Brussels, Belgium, pp: 25-27.

Alhaqbani, B., M. Adams, C. Fidge and A.H.M.T. Hofstede, 2009. Privacy-Aware Workflow Management. Queensland University of Technology, Australia.

Alhaqbani, B.S, 2010. Privacy and trust management for electronic health records. Ph.D. Thesis, Queensland University of Technology, Brisbane, Australia.

Byun, J.W. and N. Li, 2008. Purpose based access control for privacy protection in relational database systems. VLDB J., 17: 603-619. DOI: 10.1007/s00778-006-0023-0

Ferraiolo, D., D.R. Kuhn and R. Chandramouli, 2007. Role-Based Access Control. 2nd Edn., Artech House, Boston, ISBN: 1596931132, pp: 381

Fischer-Hubner, S. and A. Ott, 1998. From a formal privacy model to its implementation. Proceedings of the 21st National Information Systems Security Conference, Oct. 5-8, Arlington, VA.

He, O. and A.I. Anton, 2003. A framework for modeling privacy requirements in role engineering. Proceedings of the International Workshop on Requirements Engineering for Software Quality, Jun. 16-17, Klagenfurt/Velden, Austria, pp: 137-146.

Hu, V.C., D.F. Ferraiolo and D.R. Kuhn, 2006. Assessment of access control systems. National Institute of Standards and Technology, US.

Janse, M., H. Boland, I. Soute and K. Sheikh, 2007a. Perceived privacy in ambient intelligent environments. AMIGO.

Janse, M. D., P. Vink, I. Soute and H. Boland, 2007b. Perceived privacy in ambient intelligent environments. Proceedings of the 1st International Workshop on Combining Context with Trust, Security and Privacy (IWCCTSP' 07), New Brunswick, Canada.

Kuang, T.P., H. Ibrahim, N.I. Udzir and F. Sidi, 2011. Security extensible access control markup language policy integration based on role-based access control model in healthcare collaborative environments. Am. J. Econ. Bus. Admin., 3: 101-111. DOI: 10.3844/ajebasp.2011.101.111

Petkovic, M., D. Prandi and N. Zannone, 2011. Purpose control: Did you process the data for the intended purpose? Secure Data Manage. 6933: 145-168. DOI: 10.1007/978-3-642-23556-6_10

Tschantz, M.C., A. Datta and J.M. Wing, 2011. On the semantics of purpose requirements in privacy policies. Carnegie Mellon University.