Maryam Sepehri
Curriculum Vitae, last update February, 2020

Contents

Maryam Sepehri (maryam.sepehri@unimi.it)

Postdoc Researcher Fellow (Type A)
Dipartimento di Informatica, Giovanni Degli Antoni, University of Milan, Italy.

1 Work Experiences

- September 2018 - Present. 2 years postdoc position (type A) at Department of Computer Science, University of Milan, Italy. project title: “The Implications of Pattern Leakages on Schemes Supporting Different Types of Queries”.
- October 2017 - May 2018. Internship at David R. Cheriton School of Computer Science, University of Waterloo, Canada. Project title: “Hiding Query Pattern in Searchable Encryption Schemes”.
- September 2014 - September 2017. 3 years postdoc position (type B) at Department of Computer Science, University of Milan, Italy. project title: “Privacy-Preserving Computation in the Cloud”.
- January 2010 - March 2014. 3 years Ph.D. candidate in Computer Science with grant at Department of Computer Science, University of Milan, Italy.
- July 2006 - January 2010. Full-time faculty member at Department of Software Engineering and Information Technology, Fars Science and Research Azad University, Fars, Iran.

2 Education

- March 2014. Ph.D. student in the Ph.D. course in Computer Science with 3 years grant, at Department of Computer Science, Milan, Italy. Title of Ph.D. thesis: “Comparing Privacy-Preserving Query Processing over Outsourced Encrypted Data and Multi-Party Computation”.
  Supervisor: Prof. Ernesto Damiani, University of Mialn, Italy.
- November 2005. Master of Science (2 years course) in Software Engineering at Department of Computer Engineering, Qazvin, Iran. Thesis title: “Comparing SSADM and Object-Oriented Methodologies Using Evaluation Metrics”.
  Supervisor: Prof. Ahmad Abdollahzadeh Barforosh, Amirkabir University of Technology, Tehran, Iran.
- October 2003. Bachelor of Science (4 years course) in Software Engineering at Department of Computer Engineering, Shiraz, Iran. Thesis title: “Design and Implementation of Library Website”.

2.1 Research internships abroad and participation in international conferences and schools

The candidate has collaborated and collaborates with several international research groups, including the University of Waterloo, McGill University and the University of Ontario Institute of Technology. In the following a detailed list.

Research internships abroad

- Winter 2018 – Visiting Researcher in the David R. Cheriton School of Computer Science at the University of Waterloo, Canada, to collaborate with Prof. Florian Kerschbaum working on searching over and generally computation on encrypted data.
- Summer 2016. Visiting Researcher at School of Computer Science, McGill University, Montreal, Canada, to collaborate with Prof. Benjamin Fung, working on developing a secure proxy-based scheme in the area of Data Mining.
- September – October 2014. Visiting Researcher at Institute of Technology, University of Ontario, Oshawa, Canada, to collaborate with Prof. Patrick Hung, working on security and risk concerns in $BYOD$ (Bring Your Own Device).

Attendance at international schools

- 17-19 October 2019. "Waterloo. ai Reverse Co-op on Natural Language Processing", University of Waterloo, Canada.
- 26-30 August, 2019, "ML+ Security+ Verification Workshop", University of Waterloo, Canada.
- 23-27 September 2015. "PRACTICE, Secure and Trustworthy Computing", Bucharest (Romania). Organized by the Polytechnic Institute Bucharest in collaboration with the EU FP7 PRACTICE project.
- 01-06 July 2013. "Privacy-Aware Social Mining (MODAP)", Leysin (Swithzerland). Organized by EPFL University.
- 05-09 August 2012. "Building Trust in the Information Age", Cagliari (Italy). Organized by University of Cagliari.
- 29-03 May 2011. "ECRYPT II, Design and Security of Cryptographic Algorithms and Devices", Albena (Bulgaria). Organized by two ECRYPT II Virtual labs, namely SYMLAB and VAMPIRE.
- 04-08 July 2011. "International Summer School on Information Security and Protection", Ghent (Belgium). Organized by the Association for Computing Machinery and Ghent University.

Attendance at international conferences without talk

- 14 September, 2019, "Day of Shecurity Conference", Toronto, Canada.
- 11 September, 2019, "AWSome Day", Toronto, Canada.
- 3 June, 2019, "Blockchains and Distributed Ledger Technologies (DLTs)", University of Ryerson, Canada.
- 18 July, 2019, "AWS INNOVATE, Online Conference Global Edition (Cloud Security and Protecting information with Encryption".
- 04-06 June 2019, "ACM Symposium on Access Control Models and Technologies", ACM SACMAT, 2019, Toronto, Canada.
- 15-19 October 2019, "The 25 th ACM Conference on Computer and Communications Security", ACM CCS 2018, Toronto, Canada.
- 12-14 November 2018, "The 5th International Conference on Biomedical and Bioinformatics Engineering", ICBBE 2018, Okinawa, Japan.

2.2 Participation as speaker in national and international and conferences

- 2017 5th ACM International Workshop on Security in Cloud Computing (SCC@AsiaSCC 2017), April 2nd, Abu Dhabi, UAE, to present the paper [9].
- 2015 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 15), 20-22 August, Helsinki, Finland, to present the paper [10].
- 2013 25th International Conference on Advanced Information Systems Engineering Workshops (CAiSE 2013), 17-21 June, Valencia, Spain, to present the paper [11].
- 2013 10th VLDB Workshop, SDM 2013, August 30, Trento, Italy, to present the paper [12].
- 2012 2nd IFIP WG 2.6, 2.12 International Symposium on Data-Driven Discovery and Analysis (SIMPDA 2012), 18-20 June, Campione d'Italia, for Ph.D. presentation session.
- 2008 12th WSEAS International Conference on Computers (ICCOMP 2008), 23-25 July, Heraklion, Greece, to present the paper [13].

2.3 Awards and Acknowledgments

- September 2014 - September 2017. 3 years postdoc position (type B) at the Department of Computer Science, University of Milan, Italy.
- June 2012. Best PhD talk at the 2nd International Symposium on Data-Driven Process Discovery and Analysis, Campione d'Italia, Italy.
- January 2010 - December 2013. 3 years research grant from the Italian national funding for Ph.D. courses at the Department of Computer Science, University of Milan, Italy.

3 Professional Activities

The candidate has been PC member of international conferences and workshops like:

- 2020 IEEE International Conference on Service Computing (IEEE SCC 2020)
- 2019 IEEE International Conference on Service Computing (IEEE SCC 2019)
- 2019 IEEE International Conference on Internet of Things (ICOIT 2019)
- 2nd International Conference on Security with Intelligent Computing and Big-data Services (SIBC 2018)
- 16th International Conference on Information Technology (ICIT 2017)

The candidate has been reviewer for several peer-reviewed national and international journal and conferences.

International Journals

- Security and Communication Network (Since 2018)
- International Journal of Information Security (ISC 2013, ISC 2019)
- International Journal of Cloud Computing and Super-Computing
- IEEE Transactions on Dependable and Secure Computing (2018)

- International Journal of Knowledge and Learning (IJKL 2018)

International Conferences

- 24th International Conference on Database Systems for Advanced Applications, 2019 (As external reviewer)
- 13th International Conference on Computing Systems and Applications (AICCSA 2016)
- 13th International Conference on Data Mining (ICDM 2015)

She has been a member of research council from 2008 - 2010 at Azad University, Fars Science & Research Branch, Iran.

She also has been session chair of the UbiSafe Computing and Communications Workshop (UbiSafe), Helsinki, Finland, August 20-22, 2015.

Now, she is a member of International research and innovation Center in Intelligent Digital Systems workshop (IRIXYS) since 2016.

4 Teaching Activity and Student Tutoring

The candidate has held following courses for undergraduate students in Computer Science and & IT Department.

4.1 Teaching activity

- Lecturer, ”Data Structure and Data Management”, Winter 2018, Department of Computer Science, University of Waterloo, Canada.
- Teacher Assistant, “Laboratory of Informatics *B*”, Department of Biotechnology, 2013-2014, University of Milan, Italy.
- Teacher Assistant, “Laboratory of Programming Languages (Matlab and *C* languages)”, Department of Industry, 2013-2014, University of polytechnic, Milan, Italy.
- Teacher Assistant, “Laboratory of Informatics *B*”, Department of Pharmacy, 2012-2013, University of Milan, Italy.
- Full-Time Sessional Lecturer, “Undergraduate courses”, Department of Computer Engineering & IT, Azad University, Fars Science and Research, 2006-2010, Fars, Iran.
- Sessional Lecturer, “Undergraduate courses”, Department of Computer Engineering & IT, 2005-2006, Azad University, Marvdasht, Iran.

The main topics of the teaching courses as lecturer were Principals of Database Systems, Data Structure and Algorithms, System Analysis and Design, Data Storage and Fundamental of Software Engineering.

4.2 Student Tutoring

She has been supervisor of more than 20 undergraduate thesis focusing on different topics related to Software Engineering & IT department (The analysis, design and implementation of several websites using SSADM methodology and object oriented methodology), University of Azad, Fars Science and Research.

She collaborated with one doctoral candidate (PhD student) in her thesis titled “Applying attribute-based encryption method in IoT environment”, at Computer Science Department, University of Milan, 2015-2017.

5 Research Projects

The candidate participated/participates in the following research projects:

- Title: “PRACTICE: Privacy-Preserving Computation in the Cloud”. Coordinator: Prof. Ernesto Damiani. Financing body: European Community’s Seventh Framework Program.

  The PRACTICE project aims to build a secure framework that allows practical cryptographic technologies providing data security and privacy guarantees for all business partners interested in joint applications. This project enables European consumers to save costs by globally outsourcing to the cheapest provider guaranteeing security.

Furthermore, the candidate is a co-author of the following deliverables:

- Risk Assessment Case Study (D24.1), 2014-2015.
- Risk Aware Development and Legislative Developments in Data Protection (D31.2), 2015-2016.

  The goal of these deliverables were to develop a risk management methodology for data sharing in cloud-based services. To this purpose, we first modeled a case study of Aircraft Engine Maintenance with two types of process interactions, secure (using Homomorphic Encryption and Secret Sharing techniques) and non-secure models. We also used a quantitative estimation to measure data privacy in both process models.

- Title: “Privacy-Respecting Information Sharing”

  This project aims to show that the secure computation of differentially private set operations-intersection and intersection cardinality- is practically feasible. To this purpose, we developed a new private set intersection protocol based on homomorphic encryption where result is differentially private. The protocols has optimal communication and computation complexity as well as accuracy for a given privacy parameter. Consequently, the proposed protocols are practical for large data sets up to million of elements.

  - Deliverable: Differentially Private Two-Party Set Operations. (Paper Submitted)

- Title: “Hierarchical Classification Algorithms in Biomedical Taxonomies”

  This project aims at developing dedicated machine learning techniques to leverage the hierarchical relatedness among tasks to achieve accurate predictions, by simultaneously learning multiple tasks, or by adopting transfer learning techniques to improve the available information of individual tasks. Other issues characterizing the binary classification problems such as the integration of heterogeneous data sources,the imbalance of data labeling, the selection of negative examples, will also be addressed to improve the classification performance

- Deliverable: Analysis of Novel Annotations in the Gene Ontology for Boosting the Selection of Negative Examples. In 9th International Conference on Biomedical Engineering and Technology, ICBET 2019, Tokyo, Japan, 2019 (Paper Published).

6 Research Activity

The candidate's research activity mainly focused on the design of new privacy-preserving query processing $PPQP$ protocols over encrypted data. In particular, the candidate developed protocols efficient for executing queries adopting Secure Multi-Party Computation (SMC) and Proxy Re-Encryption (PRE) methods. She has given contributions in areas of collaborative scenarios as well as in cloud computing environment. Furthermore, she developed the designed methods in different application domains such as healthcare and air cargo chain. She investigated the development of multi-owner query processing protocols in machine learning, more specifically data outsourcing. She also focused on another interesting direction in cloud computing namely access control of the user when there are multiple users with different access permissions. Thus, she worked on design new protocols to support fine-grained access policies and policy transformation using Attribute-Based Encryption and Inner-Product Encryption Scheme. The candidate's recent work indeed focused on reconstruction attacks against persistent adversaries for schemes supporting different types of queries especially point and range queries. She also worked on private information sharing using Homomorphic Encryption methods and differential privacy.

6.1 Secure Multi-Party Computation

This area regards privacy-preserving query processing problem in multi-party computation. The candidate investigated this problem on databases where relational queries have to be executed on horizontal data partitions held by different data owners. She proposed secure multi-party computation (SMC) solutions [3, 11, 12] to compute queries over entire relation(s) by sharing data among multiple mutually distrusting parties while preserving the privacy of their sensitive data. The solutions were applied to a subset of SQL query language including Equality-test (point), Range and Equi-join queries.

- **Privacy-Preserving Equality Test Queries**
  In this context, the candidate designed a protocol for the Secure Multi-party Equality test Problem ($SMEP$), which is secure and efficient when the number of parties and the size of data increase. In [3, 11], she presented a new protocol, $B - SMEQ$ (Bucketized Secure Multi-party protocol for Equality test Queries) to address the $SMEP$ problem, which adopts a bucketization technique to reduce time complexity. The solution uses a commutative encryption scheme to avoid information being revealed among data owners. In order to make the protocol fast, the data divided into buckets in order to work only on a subset of data. To realize the bucketization scheme, a trusted third party (TTP) is involved in an initial phase. However, the TTP does not participate in the query processing, avoiding the creation of computation and communication bottleneck.

- **Privacy-Preserving Range Queries**
  This problem has been addressed by the candidate in [3, 12]. She proposed a scalable solution by transforming a range query over real numeric data in a sequence of equality test queries where each equality test resolves using $B - SMEQ$. The candidate proposed an

extension of B-SMEQ to execute privacy-preserving range queries over partitioned data in scalable manner. The proposed method exploits the relationship between range and equality queries to transform a range query in a set of equality queries. By appropriately splitting the searchable attribute, the number of equality queries is considerably reduced. Moreover, by adopting a bucketization technique which allows to work solely on a subset of data, the proposed protocol scales well when large size data are considered.

- **Privacy-Preserving Equi-join Queries**
  Most of techniques supporting $PPQP$ on SMC paradigm suffer from high computation and communication costs, and in application with high volume data (e.g., social networks) this is a crucial problem. To this end, the candidate proposed a novel SMC protocol based on bucketization and Map-Reduce techniques in [3]. The mapping phase reorders the data in a SMC scenario, in which each node (party) has data encrypted with the same key. A reduce phase is invoked after mapping to compute SMC equi-join with selection exploiting bucketization technique to reduce the computation and communication costs. Such protocol is an extension of $B-SMEQ$ that supports equality test queries on shared data [11].

Implementation: The candidate verified the scalability of the proposed protocols via some experiments implemented using Castalia simulator, a C++ based simulator to build a network of parties in order to share their data.

6.2 Cloud Security and Privacy

The candidate's research activity in cloud computing involved the study and application of $PPQP$, data sharing among users with different access rights and data outsourcing in Machine Learning area.

6.2.1 Cloud Database Querying

This part of the candidate's research activity involves the design of $PPQP$ schemes over encrypted data outsourced to the cloud. The candidate proposed protocols [9, 10] adopting proxy re-encryption technique, where a proxy is given a re-encryption key that enables it to convert encrypted data into another ciphertext of the same data using a different key.

- **Proxy-Based Protocol for Privacy-Preserving Queries**
  Due to the fact that outsourcing data on the cloud poses many challenges related to data owners and users privacy, the candidate addressed the problem of executing queries in a scenario where multiple data owners outsource their data to an untrusted cloud service provider, accepting encrypted queries coming from authorized users. She proposed a highly scalable proxy re-encryption scheme [10] so that (i) the cloud service provider can return only the encrypted data that satisfies user's query without decrypting it, and (ii) the encrypted results can be decrypted using the user's key. The proposed solution is based on $El-Gamal$ public key cryptosystem, which is fairly simple for key translation and more efficient in executing the proxy encryption/decryption operations than RSA-based schemes.

- **Efficient Proxy-Based Scheme for Data sharing on the Cloud**
  The candidate provided a secure and efficient outsourcing scheme for multi-owner data sharing on the cloud where multiple data owners outsource their data to an untrusted cloud provider [9]. The protocol allows authorized users to query the resulting database, composed of the encrypted data contributed by the different owners. It relies on a proxy re-encryption

technique and that is implemented using $El - Gamal$ Elliptic Curve (ECC) cryptosystem. The goal of the scheme was to allow authorized users to execute queries efficiently on the union of the databases they own, still maintaining the confidentiality of the data individually stored, and avoiding also that other parties and the cloud provider, executing the query, access the data. The candidate modified the proxy re-encryption scheme utilizing $El - Gamal$ encryption system.

- **Cloud-Based Technique for Air Cargo Cancellation Problem**
  One of the main problem in air cargo revenue management is the modeling of over booking and cancellation in the operation of the service chain. In fact, airline cargo companies do not impose any feed for last-minute cancellations of shipments. As a result, customers can book the same shipment on several cargo companies. Cargo companies try to balance cancellations by a corresponding volume of over booking. Toward this concern, the candidate developed a cryptographic technique [1], enabling the computation on private information of the airline customers and companies data to improve the overall service chain. The proposed protocol is based on proxy re-encryption method to mitigate the airline cargo cancellation problem while preserving the privacy of customers' data .

Implementation: The candidate verified the performance of the proposed protocols via some experiments implemented in C language using big integer function of GNU Multiple Precision (GMP) and Pairing-Based Cryptography (PBC) libraries for $El-Gamal$ and ECC cryptosystem, respectively.

6.2.2 Access Control in Cloud

This line of research aims to define fine-grained access policies over encrypted data whose enforcement can be outsourced to the cloud where the data is stored. To achieve encryption-based support of access control policies, the candidate presented a fast and secure proxy-based scheme using a variant of Inner-Product Encryption (IPE) [2, 8]. The proposed technique updates the attribute vector via a proxy server without interaction with the data owner. The proxy holds a re-encryption key to update all ciphertexts encrypted according to attribute vector $\vec{x}$ into ciphertext encrypted according to attribute vector $\vec{w}$. The candidate showed that the proposed scheme is selectively attribute-hiding secure chosen-plaintext attacks (CPA) in the standard model under the Decisional Bilinear Diffie-Hellman Problem. Moreover, she analyzed and compared the scheme with previous attribute based proxy re-encryption and inner-product encryption scheme in terms of the size of key and ciphertexts, and computation overhead. As a result, the scheme is more efficient and secure compared to several previous works, because Decrypt and Re-Decrypt algorithms require fixed pairing operations, which is more appropriate for addressing the challenge of secure data sharing among multiple users in critical applications such as healthcare.

Implementation: The candidate measured the execution time of proposed algorithm in C using Pairing-Based Crypto library for three different types of elliptic curves.

6.2.3 Data Outsourcing in Machine Learning

Due to the privacy concern in several applications in Machine learning context, it is important that data and the classifier remain confidential. In a classic privacy-preserving classification, an authorised user has private input presented as a feature vector and the server has a private input consisting of a private model. A classifier runs over the unseen features using the model to output a predication. Therefore, the user should learn the output of the predication and nothing else abut the model. To clarify the importance of privacy issue, the candidate proposed a proxy-based privacy-preserving Naive Bayes classification protocol over outsourced data residing on the cloud service provider. The protocol applied to vertically partitioned data, i.e., each data provider has a different set of attributes assuming that the class attribute of the training data is known to all data providers. Prediction was accomplished by independently estimating the probabilities at each data provider site and securely multiplying and comparing on the cloud service provider to obtain the predicted class. It is important that the model learned not reveal information to the cloud service provider. In the proposed model, each data provider collaborates to classify data miner (user) instance. The only knowledge gained by either the cloud or data miner side is the class of each instance classified. To show that the proposed protocol preserves data privacy, each data owner encrypts the computed probabilities locally using $El-Gamal$ Elliptic Curve encryption method. The principal attraction of adopting ECC is that there is no sub exponential time algorithm in solving the Elliptic curve using Elliptic Curve Discrete Logarithm Problem.

Implementation: It is planned to implement the proposed protocol using C++ language in order to analyze the time required for executing data encryption/decryption at data provider and proxy sites, the processing operations on the cloud service provider and the required time to answer the query posing by the user (data miner).

6.3 Hiding Query Pattern for schemes supporting point and Range Queries

Towards efficient search over encrypted data, various searchable encryption schemes have been proposed in the literature. While these schemes are effective in preserving the privacy of the underlying data against a snapshot attacker, they, however, leak some information during search operations due to access and query pattern leakage. Consequently, this potential privacy concern introduces general attacks by an adversary that controls the cloud service provider and hence can observe these patterns. Using some prior knowledge about data or query distribution the adversary can run simple frequency analysis attacks. While there are known, lightweight countermeasures to hide the access pattern by padding the ciphertexts, the same is not true for the query pattern or the combination of query and access pattern. Oblivious RAM ($ORAM$) can hide these patterns, but requires a superlinear cost in the size of the database and hence will become slower as data grows. Therefore, the objective of this research is to present a method to hide the query pattern of searchable encryption schemes by introducing fake queries. To this purpose, the candidate presented a query smoothing algorithm that can hide the frequency information in the query distribution by creating fake queries [4]. She showed theoretically and empirically that the proposed frequency smoothing algorithm incurs a constant overhead on $Zipf$ distributed queries, i.e. there is a constant number of fake queries for each real query independent of the data base size. The proposed algorithm not only scales better than $ORAM$ but outperforms it in practice by an order of magnitude. It also used to protect range-searchable encryption. Moreover, the algorithm can be combined with most range-searchable encryption schemes and prevents all known reconstruction attacks on encrypted range queries when applied properly.

Implementation: The candidate performed $ORAM$-based experiment by choosing the C++ implementation of $PathORAM$, available in $SEAL-ORAM$ library. She also used $Java$ for implementing the proposed query smoothing algorithm using Clusion library. Several experiments have been performed with R language to investigate the effectiveness of the algorithm as a countermeasure against query frequency analysis attacks.

7 Seminar, Talks and Poster

- April 2019. *Cryptography, Security, and Privacy (CrySP) research group*, title:"Reconstruction Attack on schemes supporting range queries ", Waterloo University, Canada.

- December 2018. Cryptography, Security, and Privacy (CrySP) research group, title:“Hiding Qery Access Pattern Leakage in keyword search techniques ”, Waterloo University, Canada.
- June 2018. *International research and innovation Center in Intelligent Digital Systems workshop (IRIXYS)*, title:“Access Pattern Leakages in Searchable Encryption”, Gargnano, Italy.
- November 2016. *International research and innovation Center in Intelligent Digital Systems workshop (IRIXYS)*, title: “Privacy-Preserving Classification in in Multi-owner Scenario”, Lyon, France.
- January 2016. *Knowledge Diffusion Network, Iranian academics*, title: “Data Sharing on the Cloud”, Shiraz University of Technology, Shiraz, Iran.
- November 2015. *Knowledge Diffusion Network, Iranian academics*, title: “Secure Equality Search on Shared Encrypted Data”, , Lyon, France.
- January 2014. *12th Multimedia Distributed Pervasive Secure Systems Workshop (MDPS)*, title: “Risk Assessment of Process-Related Data Leakage on Cloud”, Besancon, France.
- December 2013. *11th Multimedia Distributed Pervasive Secure Systems Workshop (MDPS)*, title: “Privacy-Preserving Query Processing over Outsourced Encrypted Data and Multi-Party Computation”, Lyon, France.
- January 2013. *9th Multimedia Distributed Pervasive Secure Systems Workshop (MDPS)*, title: “Privacy-Preserving Query Processing in Multi-Party Computation”, University of Messina, Scilia, Italy.
- June 2012. *2nd International Symposium on Data-Driven Process Discovery and Analysis*, title: “Privacy-Preserving Query Processing over Data Outsourcing and Multi-Party Computation Paradigm”, Campione d’Italia, Italy.
- June 2012. *8th Multimedia Distributed Pervasive Secure Systems Workshop (MDPS)*, title: “Query Processing over Outsourced Encrypted Data and Multi-Party Computation”, Lyon, France.
- December 2011. *6th Multimedia Distributed Pervasive Secure Systems Workshop (MDPS)*, title: “Privacy-Preserving Query Processing by Multi-Party Computation”, Passau, Germany.
- June 2011. *6th Multimedia Distributed Pervasive Secure Systems Workshop (MDPS)*, title: “Query Processing over Outsourced Encrypted Data”, Crema, Italy.

8 Publications

8.1 Research submitted to international peer-reviewed journals

J.1

[1] G. Gianini, S. Cimato, **M. Sepehri**, E. Damiani, and R. Asad. A Cryptographic Cloud-based Approach for the Mitigation of the Arline Cargo Cancellation Protection. *Journal of Information Security and Applications*, 2019. (Published)

J.2

[2] M. Sepehri, A. Trombetta, and **M. Sepehri**. Secure Data Sharing in Cloud Using an efficient Inner-Product Proxy Re-Encryption Scheme. *Journal of Cyber Security and Mobility* , 2018. https://Doi 10.13052/jcsm2245-1439.635. (Published)

J.3

[3] **M. Sepehri**, S. Cimato, and E. Damiani. Privacy-Preserving Query Processing by Multi-Party Computation. *Comput. J. 58(10): 2195-2212*, 2015. https://doi.org/10.1093/comjnl/bxu093. (Published)

8.2 National and international peer-reviewed conferences

C.1

[4] **M. Sepehri**, and F. Kerschbaum. Low-Cost Hiding of the Query Pattern. Submitted to *40th IEEE International Conference on Distributed Computing Systems, ICDCS 2020*, Singapore, 2020. (Submitted)

C.2

[5] B. Kacsmar, B. Khurram, N. Lukas, A. Norton, M. Shafieinejad, Z. Shang, B. Baseri, **M. Sepehri**, S. Oya, and F. Kerschbaum. Differentially Private Two-Party Set. Submitted to *5th IEEE European Symposium on Security and Privacy*, Genova, Italy, 2020. (Submitted)

C.3

[6] **M. Sepehri**, and M. Frasca. Analysis of Novel Annotations in the Gene Ontology for Boosting the Selection of Negative Examples. In *9th International Conference on Biomedical Engineering and Technology, ICBET 2019*, Tokyo, Japan, 2019. (Published)

C.4

[7] M. Frasca, **M. Sepehri**, A. Petrini, G. Grossi, and G. Valentini. Committee-Based Active Learning to Select Negative Examples for Predicting Protein Functions. In *15th International Conference on Computational Intelligence Methods for Bioinformatics and Biostatistics, Caparica, Portugal, 2018. (Published)*

C.5

[8] M. Sepehri, A. Trombetta, ***M. Sepehri****, and E. Damiani. An Efficient Cryptography-Based Access Control Using Inner-Product Proxy Re-Encryption Scheme. In* 2018 International Conference on Availability, Reliability and Security, ARES 2018, Hamburg, Germany, 2018. *(Published)*

C.6

[9] ***M. Sepehri****, S. Cimato, and E. Damiani. Efficient implementation of a proxy-based protocol for data sharing on the cloud. In* 5th ACM International Workshop on Security in Cloud Computing, SCC @ AsiaSCC 2017, Abu Dhabi, UAE, 2017. *(Published)*

C.7

[10] ***M. Sepehri**, S. Cimato, E. Damiani, and C. Y. Yeun. Data Sharing on the Cloud: A Scalable Proxy-Based Protocol for Privacy-Preserving Queries. In* 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), 20–22 August*, Helsinki, Finland, 2015. (Published)*

C.8

[11] ***M. Sepehri**, S. Cimato, and E. Damiani. A Scalable Multi-Party Protocol for Privacy-Preserving Equality Test. In* Advanced Information Systems Engineering Workshops - CAiSE 2013 International Workshops, June 17-21*, Valencia, Spain, 2013. (Published)*

C.9

[12] ***M. Sepehri**, S. Cimato, and E. Damiani. A Multi-Party Protocol for Privacy-Preserving Range Queries. In* Secure Data Management - 10th VLDB Workshop - SDM 2013, August 30*, Trento, Italy, 2013. (Published)*

C.10

[13] ***M. Sepehri** and M. Goodarzi. Leader Election Algorithm Using Heap Structure. In* 12th WSEAS International Conference on Computers (ICCOMP 2008)*, Heraklion, Greece, 2008. (Published)*

C.11

[14] ***M. Sepehri**, A. Abdollahzadeh, M. Sepehri, and M. Goodarzi. Comparing Object Oriented and SSADM Methodologies Using Evaluation Parameters. In* The International Conference on Software Engineering Research & Practice (SERP'07),June 25-28*, Las Veges, Nevada, USA, 2007. (Published)*

C.12

[15] ***M. Sepehri**, A. Abdollahzadeh, M. Sepehri, and M. Goodarzi. The Impact of Quality Factors on the Success of Software Development Methodologies. In* European Computing Conference*, Atlanta, Greece, 2007. (Published)*

C.13

[16] ***M. Sepehri**, M. Dehghan, and A. Haghighat. A Scheme for an RPC Mechanism Using Election Algorithm. In* The International Multi Conference in Computer Engineering (IMCSE 2005)*, June 27-30*, Las Vegas, Nevada, USA, 2005. (Published)