# An Overview of Data Privacy in Multi-Agent Learning Systems

Kato Mivule
Computer Science Department
Bowie State University
Bowie MD, USA
Mivulek0220@students.bowiestate.edu

Darsana Josyula, Claude Turner
Computer Science Department
Bowie State University
Bowie MD, USA
djosyula@bowiestate.edu, cturner@bowiestate.edu

**Abstract— Public and private sector entities continuously produce, store, and transact in large amounts of data. However, combined with the growth of the internet, such datasets get stored and accessed on multiple devices, locations, and across the globe. Therefore, the necessity for autonomous agents that can learn across distributed systems to extract knowledge from large datasets while at the same time taking into account data privacy considerations while interacting with other agents remains a challenge. In this paper, we endeavor to provide an overview of data privacy in multi-agent learning systems, while at the same time highlighting current challenges and future areas of work and research.**

**Keywords: Multi-Agents; Inductive Learning; Data Privacy**

## I. INTRODUCTION

Public and private sector entities constantly generate, collect, and transact in large quantities of data (big data). However, with the growth of the internet, such datasets are stored and retrieved across numerous devices, and localities, across the globe. Therefore, there is necessity for artificial intelligence (AI) agents that can learn across distributed systems to extract knowledge from large datasets while at the same time taking into consideration data privacy and security issues in relation to other independent agents.

The problem of privacy and security in multi-agent systems has been an area of research interest for some time. As of 1996, Forner (1996) observed that the handling of sensitive data in multi-agent systems was still problematic due to privacy enhancing design challenges in multi-agent systems; Forner (1996) suggested cryptographic solutions to deal with privacy issues in multi-agent systems [34]. Wong et al. (2000) further addressed the problem of security and trust in multi-agent systems and proposed a security and trust architecture that ensured that agents do not act in contradiction to their designed purpose and that agents self-authenticate to ensure trust by retaining traits of correct naming and matchmaking services, secure communication channels, secure delegation when acting on behalf of other agents, and accountability [35]. However, Yu et al. (2003), succinctly and aptly observed that in multi-agent systems, privacy may have various meanings and importance for different agents; and that when designing architectures for multi-agent systems, there should be room for a diversity of perceptions and views on privacy [36]. In this article, we take this conceptual approach to privacy preservation in multi-agent systems. It is very difficult to define precisely what privacy is and therefore it becomes problematic to create a generalized solution to privacy complications.

As Spiekermann (2012) observed, one of the challenges of engineering privacy is that privacy is a fuzzy concept often confused with security, and, as such, difficult to implement [40]. Additionally, Friedewald et al. (2010) in their research on the legal characteristics of privacy, made a critical observation, that privacy is an evolving and shifting complex multi-layered concept, described differently by different people [41]. To add to this point, Katos et al. (2011) noted that privacy is a human and socially driven distinctive made up of human mannerisms, perceptions, and opinions [39]. Therefore, definitions for data utility get taken in the same light as privacy that is, data utility is the concept of how useful a privatized dataset is to the user of that particular privatized dataset [11]. Furthermore, despite various approximation methods that have been developed and designed to quantify data utility, researchers have noted that data utility varies from one scenario to the next, and, as such, problematic to have a generalized data utility gauge [12]. We believe that it is imperative that such fuzzy definitions of privacy and utility be taken into consideration when engineering privacy in multi-agent systems to avoid the pitfall of a generalized one-size-fits-all model.

Moreover Ramchurn et al. (2004) gave a detailed overview of the problem of trust in multi-agent systems due to the interactions that agents have in such environments; they observed three main aspects of problematic areas of trust in multi-agent systems: (i) how to engineer protocols for multi-agent interactions, (ii) how would agents decide who to interrelate with, and (ii) how agents decide when to cooperate with each other [37]. In their survey of security issues in multi-agent systems, Jung et al. (2012) made an important observation that multi-agent systems have become critical to autonomous computing today and therefore matters of security such as access control and trust are issues that need to be addressed [38]. This argument is further exemplified by Martins et al. (2012) in their review of security mechanisms in mobile agents, by pointing out the security threats that multi-agents face the need for agents to conform to the three canons of privacy and security, namely, confidentiality, accessibility, and integrity [26]. Lastly, Nagaraj (2012) observed that the analysis of security requirements for multi-agents, and, in this case, privacy requirements, is often neglected during the requirements phase of designing multi-agents [25]. Therefore, we believe that it is essential that any architecture, design, and

 ISBN: 978-1-61208-273-8 

engineering of multi-agent systems seriously take privacy and security issues into consideration.

A number of data privacy enhancing algorithms have been suggested. Yet adopting the proposed algorithms for privacy preservation among autonomous agents remains a challenge. In multi-agent systems, communication and learning among the various autonomous agents involve dealing with privacy and security issues when one considers what sensitive and personal information autonomous agents can or cannot share. An example would include how multi-agents would transact data in a health care system in which compliance to Federal and state laws require that personal identifiable information (PII) be kept confidential. Although a number of ongoing challenges exist for multi-agents in a distributed environment, in this paper we focus on data privacy issues in multi-agent learning systems as presented in current literature. The remaining part of the paper is ordered as follows: In Section II, we take a look at background of multi-agents as described in the literature. Section III deals with how multi-agents learn while in Section IV, we look at current data privacy issues in multi-agent learning systems. In Section V, we outline a conceptual architecture for privacy preserving multi-agent learning systems, and, finally, in Sections VI and VII, we provide our conclusion while highlighting future areas of research.

## II. BACKGROUND

Agents: Wooldridge (2003) defined agents as computer systems that are located in a particular environment with the capability of independent and autonomous action in that particular environment so as to achieve the goals of what they were designed to do [1]. Multi-Agents: Wooldridge (2003) further described multi-agents as a group of autonomous agents combined into one system, independently solving simpler problems while communicating with each other to accomplish bigger and complex objectives [1]. Multi-agent systems (MAS): Da Silva (2005) noted that multi-agent systems are formed to deal with complex applications in a distributed systems environment. Da Silva (2005) also observed that examining data in distributed environments is a difficult problem since agents face several restrictions; for example, limited bandwidth in wireless networks and privacy issues with sensitive data [2]. MAS characteristics: However, Albashiri (2010) illuminated in his dissertation that MAS are defined by the following three traits [3]: (i) MAS essentially have to stipulate proper communication and interfacing protocols to efficiently connect with other agents; (ii) MAS need to be open and distributed with no previous information of other agents and their activities; (iii) MAS may consist of conceivably diverse agents that are distributed in that particular environment and acting independently or cooperatively to accomplish an objective. Machine Learning: Machine learning was described earlier by Samuel (1959) as the ability to encode and train computers to learn from experience and ultimately eliminate the necessity for the much exhaustive programming effort [4]. However, a more concise and commonly used formal description was given by Tom Mitchel (1997): "A computer program is said to learn from experience **E** with respect to some class of tasks **T** and performance measure **P**, if its performance at tasks in **T**, as measured by **P**, improves with experience **E**" [5].

Big data: According to IBM, a private sector business leader in handling large amounts of data, 'big data' is a collection of large quantities of data that hold the following four characteristics, (i) volume, concerned with the large amounts of data, (ii) velocity, which has to do with the utilization of data as it is being produced, (iii) variety, concerned with various data types, from text, numeric, image, video, and sound, just to mention a few, (iv) veracity, as in such data must be authentic and secure for transaction [6]. Data privacy and security: Pfleeger et al. (2006), identified data privacy as a controlled disclosure in which an entity decides when and to whom to disclose its data, while security has to do with access control, as in who is allowed legitimate access to data and systems [8]. The three aspects of information security are further described by Pfleeger et al. (2006) as: (i) confidentiality, ensuring the concealment and privacy of data and systems, (ii) availability, ensuring the availability of data and systems at all times, and lastly, (iii) integrity, ensuring that data and systems are altered by only the authorized [8]. Data de-identification is the exclusion of personally identifiable information (PII) from a data set [9, 10]. PII attributes are properties that uniquely identify an individual; an example includes social security number. Data utility versus privacy is the concept of how beneficial a privatized dataset is to the user of that dataset. Achieving a balance between privacy and utility needs remains an intractable problem requiring trade-offs [11, 12, 13, 14].

## III. LEARNING IN MULTI-AGENT SYSTEMS

Researchers have been fascinated by multi-agent learning for some time, and although a number of learning approaches have been proposed, in this paper we focus on two learning methods from literature to highlight the need for integration of data privacy principles in multi-agent learning systems. In an extensive review, Davies (1994) noted that Inductive Logic Programming (ILP) techniques were deployed as software agents for first order knowledge discovery in distributed databases [7]. Davies (1994) described how users are able to instruct a group of agents to discover information from particular databases. In general, a user presents an objective, and then the agents cooperate with other agents to accomplish this goal. Davis (1994) employed a combined approach with empirical first order inductive learning (inductive logic programming), data mining, and software multi-agent systems [7].

Moreover, Davies et al. (1995) explained in additional detail how agents learn in stages while discovering information in a distributed environment [15]: First phase: agents gather data in a centralized location. Second phase: agents interchange information while learning on resident data. Third phase: agents learn locally and then distribute results among fellow agents, after which the results are retuned and absorbed by other agents based on their own

 ISBN: 978-1-61208-273-8 

data and knowledge. Davies et al. (1995) categorized agents in a distributive environment as: Non Distribution Agents: agents learn from local training examples. Incremental Theory Revision Agents: agents learn a local theory from existing training examples, and then share the learnt theory to the next agent. Simple Knowledge Integration Agents: agents learn a local theory, get tested on the training examples, and after comparison of results, the agent with the best theory is chosen. Theory Revision and Simple Knowledge Integration Agents: multiple agents learn a local theory and distribute the learned local theories to all the other agents. At this point each local agent then revises the received theories to fit local data, after which the agent tests each theory with the local training set and chooses the best theory after comparison of results [15].

Support Vector Machines (SVM), Multi-agents, and Incremental Learning: A description of how SVM based agents learn was given by Caraga et al. (2002) in which SVM based incremental learning involves an agent working on a dataset $\mathbf{D_1}$ to produce a group of support vectors $\mathbf{SV_1}$, the results of $\mathbf{SV_1}$ are then added to dataset $\mathbf{D_2}$ to produce dataset $\mathbf{D_2'}$; after, another SVM based learning agent processes dataset $\mathbf{D_2'}$ generating $\mathbf{SV_2}$ results. The process continues, utilizing datasets $\mathbf{D_1}$ and $\mathbf{D_2}$, until a resulting classifier is learned, such that $\mathbf{D = D_1 \cup D_2}$ [16]; where $\mathbf{D_1}$ and $\mathbf{D_2}$ are datasets, $\mathbf{SV_1}$ and $\mathbf{SV_2}$ are a group of produced support vectors. However, in their paper on the subject of SVM multi-agents and refuse data Ontanon et al. (2005) expounded on the cooperative learning of SVM multi-agents that utilized an ensemble effect for learning, by basically engaging in negotiating activities to improve individual agent and collective committee agent performance. Such agents have the capability of self-assessment and making decisions that some data used for learning is not needed [17]. Multi-agents situated in a distribution environment engage in communication and transaction of data and therefore questions of how such autonomous agents can learn by integrating data privacy and security principles remains a challenge.

## IV. PRIVACY ISSUES IN MULTI-AGENT SYSTEMS

Privacy preserving architectures for multi-agent systems have been proposed but they mainly focus on access control rather than confidentiality. For instance, Cissee (2003) proposed a privacy preserving information filtering agent based architecture in which private or sensitive information was neither controlled by the user or provider of data gathering service but user and provider profiles could be shared between the two parties based on a trust relationship and thus filter any untrusted party [18]. In addition, Crepin et al., (2009) proposed specification for Hippocratic multi-agent systems in which each transaction of data requires a provider's consent, limited collection of data, limited use of data, limited disclosure of data, limited retention of data, safety, and openness of data transactions by the multi-agents [19]. Another instance of access control trade-offs was the proposal by Leaute et al. (2009) in which multi-agents employ constraint satisfaction techniques, often used in resource allocation problems, and might consider trade-offs of their privacy constraints and decisions in the privacy preservation process [20]. Also, Such et al. (2012), proposed a self-disclosure system in which autonomous agents make decisions whether to disclose personal attributes to other agents mirrored after human relationships in which cost benefits are considered before disclosing private information [21]. Challenges of privacy preservation in multi-agent systems still remain an open research problem. Such et al. (2012), observed that multi-agents are vulnerable to three information-related activities: (i) information collection in which agents collect and store data about an individual, (ii) information processing whereby agents modify data that has been collected, and finally (iii) information dissemination, whereby agents publish data [22].

Klusch et al. (2003) observed then that one of the major challenges with distributed data mining was the issue of autonomy and privacy of agents in a distributed environment [23]. Albashiri (2010) indicated yet another challenge that multi heterogeneous agent systems, have to specify suitable communication and interfacing protocols and must be decentralized with new agents connecting at will by adapting to the communication protocol [3]. However, Rashvand et al. (2010) showed that multi-agent security requirements might appear in three categories: (i) service-agent protection, in which agents are protected from external threats; (ii) system vulnerability protection, in which the platforms and agents are protected from insecure internal processes; lastly, (iii) protective security services, in which the main objective of an agent is to provide security [24].

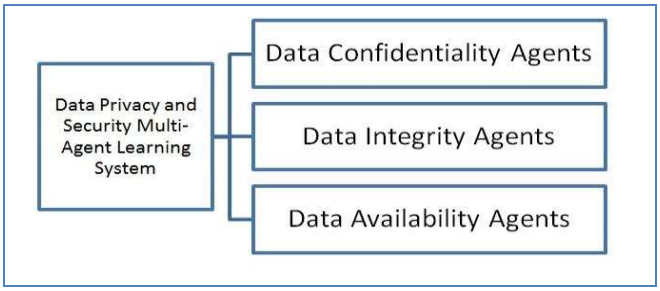


Figure 1. Conceptual Categories of Data Privacy Multi-agents.

On the issue of software engineering security requirements, Nagaraj (2012) indicated that security concerns such as, agent misbehavior (e.g., denial of service attacks), are still not taken into consideration while designing multi-agent systems and that if attempts are made, tackling such security issues in multi-agent systems tends to happen after the design phase [25]. Additionally, Martins et al., 2012) noted that for secure mobile agent communication, key security concerns of authentication, confidentiality, and integrity must be taken into consideration by multi-agents [26]. Krupa et al. (2012) suggested the utilization of 'Privacy Enforcing Norms' in which agents learn a set of acceptable privacy agent social behavior and when such Norms are violated, other fellow agents are notified and penalties to the offending agent are issued [27]. Lastly, Krupa (2012) observed that implementing privacy for multi-agents in a

 ISBN: 978-1-61208-273-8 

distributed system is still problematic and a challenge, whereby, (i) agents have to learn how to sense privacy violations; (ii) how such a multi-agent system can be managed without centralization to deter and halt confidentiality abuses; (iii) and the need to find flexible solutions to the inapplicability of most existing privacy enhancement methodologies [28].

## V. An Architecture for Privacy Preserving Multi-agent Learning System

Observations from our literature review on privacy issues in multi-agents, show that a number of research challenges still exist, mainly, how to integrate privacy and security principles in multi-agent learning architectures. In our conceptual contribution, we suggest an organizational structure as shown in Figure 1, that categorizes privacy preserving multi-agents as: (i) Confidentiality agents, those that handle data concealment and privacy; (ii) Integrity agents, those that handle non repudiation in data transactions, ensuring that data is altered by only authorized agents; and lastly, (iii) Availability agents, these are agents that ensure that all other agents are available for communication and that their resources are available at all times, by preventing and reporting attempted denial of service attacks.

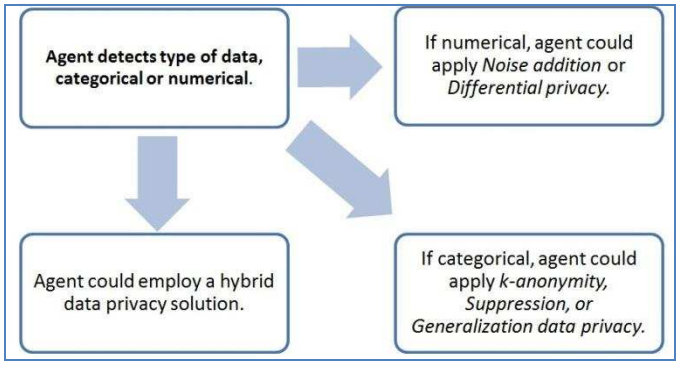


Figure 2. A data privacy procedure selecting autonomous agent.

In this way, the data privacy multi-agent system would conform to the three aspects of data privacy and security, that is, confidentiality, integrity, and availability. Communication between these multi-agents in the various levels of the architecture is a must. Secondly, we could have various data privacy roles under the specified major categories; for instance, since our focus in this paper is on data privacy preservation, under the Confidentiality category, we suggest data privacy algorithm selector multi-agents that would autonomously check what type of dataset that it is handling (categorical or numerical) as shown in Figure 2. If the data is numerical, then an agent applies Noise addition or Differential privacy data privacy algorithms [30]. If the data is categorical, the agent applies k-anonymity algorithm, Suppression, or Generalization data privacy algorithms [31, 32] on that dataset. Another agent could be employed for a hybrid solution. A different agent measures and reports on the data utility of the privatized dataset. Additionally, in this suggested framework, under the confidentiality multi-agent, we could have privacy and utility trade-off agents as shown in Figure 3. These agents would ensure the privacy and utility of privatized datasets, first, by outlining the various levels of parameters in the data privacy process.

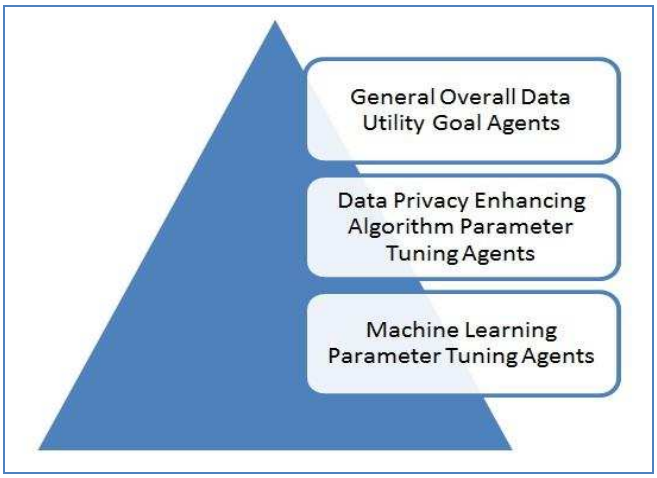


Figure 3. Hierarchical view of Parameter Tuning Agents

These agents could belong to different groups based on the parameters in the data privacy process as shown in Figure 4. General overall data utility goal agents: these would ensure that the general utility or the overall goal parameters like accuracy, currency, and completeness are attained [30].

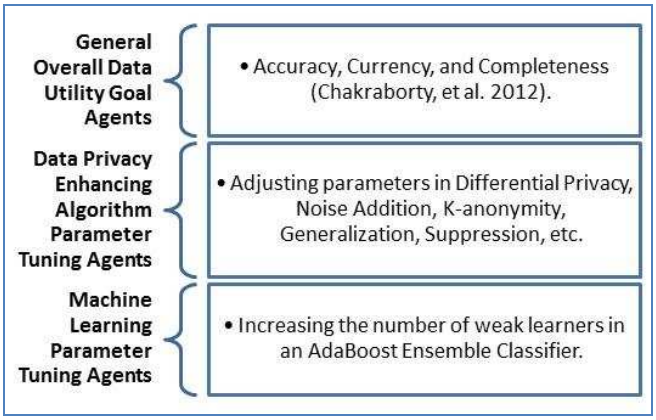


Figure 4. Functionalities of the various Parameter Tuning Agents

In this case, agents would ensure how accurate, how current, and how complete a privatized dataset ought to be. The data privacy enhancing algorithm parameters tuning agents: These agents would be responsible for autonomous adjustment and fine-tuning of parameters in the selected data privacy algorithm to ensure that not too much privacy is added while data utility diminishes. Finally, the machine learning parameter tuning agents: these agents would make adjustments to the parameters of the machine learner, such as increasing the number of weak learners. Even when multi-agents fully apply data privacy algorithms on data, the question of how such autonomous agents would have to

 ISBN: 978-1-61208-273-8 

learn to deal with the intractable problem of privacy versus utility, as illustrated in Figure 5; and how to make the trade-offs, remains open for further research.

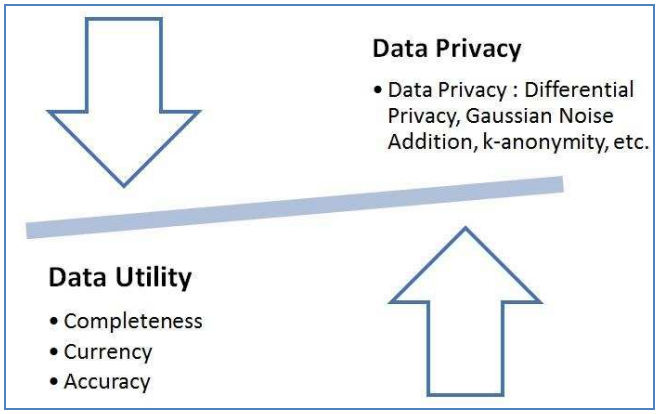


Figure 5. Trade-offs between privacy and utility are sought.

To illustrate this point, we added Differential privacy to a democratic political donation dataset, made public by the US Federal Election Commission and available online [33].

TABLE I. ORIGINAL DATA BEFORE AND SYTHETIC DATA AFTER PIVACY ENHANCEMENT

| Original Data | Data after Differential Privacy |
|---|---|
| 100 | 126.46 |
| 100 | 122.72 |
| 100 | 145.16 |
| 25 | 106.57 |
| 5 | 66.04 |
| 5 | 69.41 |
| 100 | 131.59 |
| 30 | 62.32 |
| 50 | 123.38 |
| 30 | 99.22 |

Our goal was to create a synthetic dataset that met the requirements of differential privacy so as to conceal donations made by individuals; and while that was possible our results showed that the privacy added was at the cost of data utility. For instance, as shown in Figure 6, someone who gave a donation of US $25 is reported in the privatized database as giving US $106.57. While concealment is provided, the utility of that data diminishes.

Therefore, finding the optimal balance between privacy and utility remains a challenge for multi-agents. How autonomous agents could be trained to learn to achieve to such optimality and make trade-offs in the privacy versus utility challenge remains an open question for further investigation.

## VI. CONCLUSION

In this article, we have endeavored to give a preliminary overview on privacy preservation in multi-agent learning systems in a distributed data systems environment. Our review of multi-agent data privacy issues from literature shows that the intractable problem of privacy in distributed data mining and machine learning is still a challenge with questions such as how can multi-agents in a distributed environment keep their autonomy and ensure privacy of data without disclosure of sensitive and personal information. The need for intelligent multi-agents that can learn how to discern private and sensitive data, and ensure confidentiality while communicating with other agents remains a challenge.

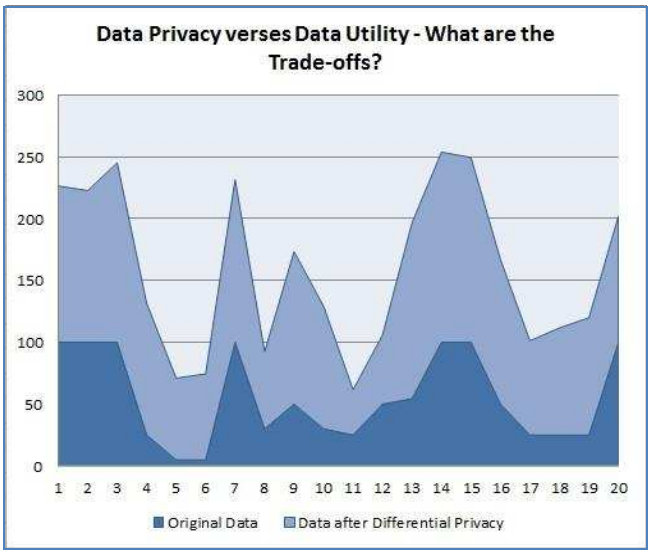


Figure 6. Trade-offs between privacy and utility are sought.

While a number of data privacy algorithms have been designed, it is important to note that they are not autonomous and do not act independently in a given environment, therefore the challenge is how to adapt such data privacy and utility algorithms for multi-agent systems. How agents can keep their autonomy, ensure privacy and confidentiality while at the same time adapting to various communication and interfacing protocols, remains a research question to be further pursued for various tailored privacy enhancing solutions. Research in data privacy enhancing algorithms is still a wide open area and applications of such data privacy algorithms in autonomous multi-agent systems still remains a challenge.

## VII. FUTURE WORK

For future work, we plan to implement our conceptual privacy preserving multi-agent learning architecture, run simulation tests including automated software prototype, identify a data privacy and utility taxonomy for the prototype, and generate empirical results to map out the optimal balance between privacy and utility needs for various data privacy scenarios.

## ACKNOWLEDGMENT

Special thanks to the Computer Science Department at Bowie State University for all the assistance in making this work possible.

 ISBN: 978-1-61208-273-8 

## REFERENCES


[1] M. Wooldridge, "An Introduction to Multi-Agent Systems." Chichester, England: John Wiley and Sons, 2003, ISBN-10: 0470519460.

[2] J.C. Da Silva, C. Giannella, R. Bhargava, H. Kargupta, and M. Klusch, "Distributed data mining and agents", Eng Appl Artif Intell, pages 791–807, 2005.

[3] K.A. Albashiri, "An investigation into the issues of Multi-Agent Data Mining", Dissertation, University of Liverpool, 2010

[4] A.L. Samuel, "Some studies in machine learning using the game of checkers". IBM Journal. Res. Dev. 3, 3, pages 210-229, 1959. DOI=10.1147/rd.33.0210

[5] T. Mitchell, " Machine Learning", McGraw Hill. ISBN 0-07-042807-7, page 2, 1997.

[6] IBM, "Big Data", Online, [Retrieved: March, 2013] http://www-01.ibm.com/software/data/bigdata/

[7] W. Davies, "Agent-Based Data-Mining", First Year Report, University, 15 August 1994, Online, [Retrieved: March 2013] http://www.agent.ai/doc/upload/200403/davi94_1.pdf

[8] C.P. Pfleeger and S.L. Pfleeger, "Security in Computing" (4th Edition). Prentice Hall PTR, Upper Saddle River, NJ, USA, pages 10, 606, 2006.

[9] US Department of Homeland Security, "Handbook for Safeguarding Sensitive Personally Identifiable Information at The Department of Homeland Security", October 2008. Online, [Retrieved February, 2013] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf

[10] E. Mccallister, and K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information ( PII ) Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-122, 2010.

[11] V. Rastogi, S. Hong, and D. Suciu, "The boundary between privacy and utility in data publishing", VLDB, September pp. 531-542, 2007.

[12] M. Sramka, R. Safavi-Naini, J. Denzinger, and M. Askari, "A Practice-oriented Framework for Measuring Privacy and Utility in Data Sanitization Systems", ACM, (EDBT' 10) Article 27, 10 pages, 2010. DOI=10.1145/1754239.1754270

[13] S.R. Sankar, "Utility and Privacy of Data Sources: Can Shannon Help Conceal and Reveal Information", Information Theory and Applications Workshop (ITA), pages 1-7, 2010 .

[14] R.C. Wong, et al, "Minimality attack in privacy preserving data publishing." VLDB, pages 543-554, 2007.

[15] W. Davies, and P. Edwards, "Distributed learning: An agent-based approach to data-mining". In working notes of ICML'95, Workshop on Agents that Learn from Other Agents, 1995.

[16] D. Caragea, A. Silvescu, and V. Honavar, "Agents that learn from distributed and dynamic data sources." In Proceedings of the Workshop on Learning Agents, pages 53-61, 2000.

[17] S. Ontañón, and E. Plaza, "Recycling data for multi-agent learning". In Proceedings of the 22nd international conference on Machine learning (ICML '05). ACM, pages 633-640, 2005.

[18] R. Cissée, "An architecture for agent-based privacy-preserving information filtering." In Proceedings of 6th International Workshop on Trust, Privacy, Deception and Fraud in Agent Systems, 2003.

[19] L. Crepin, Y. Demazeau, O. Boissier, and F. Jacquenet, "Sensitive data transaction in Hippocratic multi-agent systems." Engineering Societies in the Agents World IX, pages 85-101, 2009.

[20] T. Léauté, and B. Faltings, "Privacy-Preserving Multi-agent Constraint Satisfaction", International Conference on Computational Science and Engineering, Vol. 3, pages 17-25, 2009.

[21] JM. Such, A. Espinosa, A. GarcíA-Fornes, and C. Sierra, "Self-disclosure decision making based on intimacy and privacy." Journal of Information Sciences Vol 211, 2012, pages 93-111.

[22] JM. Such, A. Espinosa, A. GarcíA-Fornes, and C. Sierra, "A Survey of Privacy in Multi-agent Systems", Knowledge Engineering Review, in press, 2012.

[23] M. Klusch, S. Lodi, and G. Moro, "Issues of agent-based distributed data mining.", In Proceedings of the second international joint conference on Autonomous agents and multiagent systems, ACM, pages 1034-1035, 2003, DOI=10.1145/860575.860782

[24] H.F. Rashvand, K. Salah, J.M.A Calero, L. Harn: "Distributed security for multi-agent systems - review and applications". IET Inf. Secur. 4(4), pages 188–201, 2012.

[25] S. V. Nagaraj, "Securing Multi-agent Systems: A Survey." Advances in Computing and Information Technology, pages 23-30, 2012.

[26] R.A. Martins, M.E. Correia, and A.B. Augusto, "A literature review of security mechanisms employed by mobile agents," Information Systems and Technologies (CISTI), 7th Iberian Conference, pages 1-4, 2012.

[27] Y. Krupa and L. Vercouter "Handling privacy as contextual integrity in decentralized virtual communities: The PrivaCIAS framework." Web Intelligence and Agent Systems, pages 105-116, 2012.

[28] Y. Krupa, "PrivaCIAS: Privacy as Contextual Integrity in Decentralized Multi-Agent Systems." PhD dissertation, Université de Caen, 2012.

[29] S. Chakraborty, Z. Charbiwala, H. Choi, KR. Raghavan, and MB. Srivastava, "Balancing behavioral privacy and information utility in sensory data flows." Pervasive and Mobile Computing, Volume 8, Issue 3, Pages 331–345 2012.

[30] C. Dwork, "Differential Privacy", Automata, Languages and Programming, Lecture Notes in Computer Science, Springer, Vol. 4052, pages 1-12, 2006.

[31] V. Ciriani, S.D. Di Vimercati, S. Foresti, and P. Samarati, "Theory of privacy and anonymity". In Algorithms and theory of computation handbook (2 ed.), pages 18-18, Chapman and Hall/CRC, 2010, ISBN:978-1-58488-820-8.

[32] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression", IEEE Symp on Research in Security and Privacy, pp. 384–393, 1998.

[33] US Federal Election Comission, Campaign Finance Disclosure Portal, Online, [Retrieved: March 2013] http://www.fec.gov/pindex.shtml

[34] L.N. Foner, "A security architecture for multi-agent matchmaking." In Proceeding of Second International Conference on Multi-Agent System, Mario Tokoro. Pages 80-86, 1996.

[35] C.H. Wong, and K. Sycara. "Adding security and trust to multiagent systems." Applied Artificial Intelligence Vol. 14, no. 9, pages 927-941, 2002.

[36] E. Yu, and L. Cysneiros. "Designing for Privacy in a Multi-agent World." Trust, Reputation, and Security: Theories and Practice, pages: 259-269, 2003.

[37] S.D. Ramchurn, D. Huynh, and N.R. Jennings. "Trust in multi-agent systems." The Knowledge Engineering Review Vol. 19, no. 1, pages 1-25, 2004.

[38] Y. Jung, M. Kim, A. Masoumzadeh, and J.BD. Joshi. "A survey of security issue in multi-agent systems." Artificial Intelligence Review, Vol. 37, no. 3, pages 239-260, 2012.


 ISBN: 978-1-61208-273-8 

[39] V. Katos, F. Stowell, and P. Bednar, "Surveillance, Privacy and the Law of Requisite Variety", Data Privacy Management and Autonomous Spontaneous Security, Lecture Notes in Computer Science Vol. 6514, pages 123–139, 2011.

[40] S. Spiekermann, "The challenges of privacy by design," Communications of the ACM, vol. 55, no. 7, page 38, 2012.

[41] M. Friedewald, D. Wright, S. Gutwirth, and E. Mordini, "Privacy, data protection and emerging sciences and technologies: towards a common framework," Innovation: The European Journal of Social Science Research, vol. 23, no. 1, pp. 61–67, Mar. 2010.

 ISBN: 978-1-61208-273-8 