Addressing the Terms-of-Service Threat
Client-side Security and Policy Control for Free File Storage Services

Geir M. Køien and Vladimir A. Oleshchuk
University of Agder, Institute of ICT, Grimstad, Norway

Keywords: Public Cloud Services Terms-of-Service, Producer-consumer Asymmetry, Conflicting-incentives, Content Ownership, Security and Privacy, Trust, Policy Control, Reputation, Presentation Layer Manager.

Abstract: In this paper we describe and identify the so-called terms-of-service (ToS) threat. This threat is concerned with asymmetry in the power between a service producer (SP) and the service consumer (SC) and is expressed in ToS which allows the SC to change the ToS at will. Our context is the free file synchronization services, and we will analyze the relationships between the service producer and the service consumer. There are pronounced control asymmetries and potential conflicts of interest between the parties, including user privacy and content ownership control. Our proposal for addressing these problems hinges on a two pronged approach, including defining a service policy manager surveillance tool and a client side presentation manager to enforce local security and privacy policies. Our Umbrella Architecture is still very much work in progress, but we are optimistic about usefulness the approach.

1 INTRODUCTION

In this paper we investigate potential solutions to the problem now known as the *terms-of-service (ToS)* threat (Schneier, 2013). This threat emerges when the terms of service is formulated such that it may be changed unilaterally by the service producer. This can cause conflicts as was highlighted by the resent Instagram debacle (Thomson, 2012), where Instagram changed its terms of service to allow itself the right to sell user photos. In this case Instagram was forced to revise the change to its ToS after a public outcry, but it turns out that many of the "free" internet services do contain similar terms of service.

We specifically investigate the ToS threats that may arise in the context of free file storage and synchronization services. We analyse the power relationships between the service producer and the service consumer and we investigate the conflict of interests inherent in these agreements using the Conflicting Incentives Risk Analysis (CIRA) model (Rajbhandari and Snekkenes, 2012).

We propose to address the ToS threat by a combination of several measures in what we call the **Umbrella Architecture**. The main part consists of a client-side *presentation layer security manager (PLaSM)* which will protect the user content. The PLaSM will provide a set of security protection features and these will be available at all times for the user. These will as a minimum include file encryption and file integrity services.

The other components are a *policy monitoring agent (PoMA)* and a *reputation manager (ReMa)*. The PoMA will monitor the ToS and will alert the consumer in case of changes and the reputation manager will gather information about the reliability and trustworthiness of the SP. The PoMA and the ReMa may also trigger actions, called strategies in CIRA parlance. These actions will then be carried out by the PLaSM. The net result will be improved security and privacy for user content stored by cloud file storage services.

2 ANALYSIS OF THE TERMS-OF-SERVICE THREAT

2.1 Background

Needless to say for a free service, but the offering party obviously gets to dictate the premises of the ToS. There is of course a larger societal context that the SP must take into account, both with respect to legal requirements and with respect to customer reactions. In (Braman and Roberts, 2003) the authors

M. Køien G. and A. Oleshchuk V..
Addressing the Terms-of-Service Threat - Client-side Security and Policy Control for Free File Storage Services.
DOI: 10.5220/0004520205620569
In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science* (CloudSecGov-2013), pages 562-569
ISBN: 978-989-8565-52-5

discusses the legal aspects of ToS in the context of an ISP. The paper is US centric, but the general conclusions should hold in most jurisdictions.

The agreements are written in a language intended for lawyers rather than laymen. Furthermore, the SC generally has little specific knowledge about his/her rights to start with. So, informally, we summarize the ToS threat as the following:

- ToS statements are not very readable to the layman (read: ToS are seldom read)
- ToS are subject to unilateral change by the SP (and the notice could well go unnoticed)
- ToS regulate rights to the contents stored by the SP, and this may seriously affect the SC content ownership rights and SC privacy.

2.2 Security and Privacy Aspects

2.2.1 Accountability and Availability

Accountability is an important aspect for almost all cloud based services. Big service producers like Apple, Google, Microsoft, Amazon, Dropbox etc. are generally reputable organizations, and we may assume that they will provide reasonable services and be accountable for them. Smaller outfits may or may not be reputable, and in the wake of a bankruptcy or similar it will be anybodies guess as to how well behaved they will be. However, the catch is *playing by the rules*, which are those captured in the ToS. As demonstrated by the Instagram case the companies exists in a societal context, and this may prevent a company from abusing their rights.

Availability is another important aspect. It is of course purported to be a major benefit of cloud storage and for the file synchronization services one will usually have local access to the data anyhow. In our context we have decided not to pursue availability further, but note that this aspect has been addressed in the context of paid-for services (Bowers et al., 2009).

In our context we have decided not to address the accountability and availability aspects directly. That is, we assume that the required minimum of accountability and availability features are already present in the provided services.

2.2.2 Privacy, Identification, Authentication, Integrity and Confidentiality

The identification used in most of the services is based on email addresses. These are not particularly privacy sensitive, although we want to avoid unnecessary exposure. Identity privacy itself is a concern, although not the primary privacy concern her. We note that the authentication schemes for free service seems not to be particularly strong, but with additional data protection they may be adequate. This needs to be verified. Otherwise, we note that privacy has many facets and that one correspondingly must have a multifaceted approach when counteracting and mitigating privacy problems (Oleshchuk and Køien, 2011).

In (Subashini and Kavitha, 2011) the authors outline a set of security issues in delivery models in cloud computing. These issues are mostly concerned with enterprises using paid-for cloud services, but we note that many of the concerns are similar. Another paper which investigates these issues is (Zhao et al., 2010) and this paper is interesting in that it distinguishes between different deployment models. With respect to our case we note that the consumer will not have much influence upon the chosen model, apart from what can implement at the client side. Another interesting paper is (Bernsmed et al., 2011) in which there is an attempt at defining service level agreements (SLA) for cloud security. Our context is different and so the consumer will not be able to negotiate SLA arrangements, but is rather left with a ToS that he/she cannot negotiate.

It should be evident that we need both data integrity and data confidentiality. The SC needs to ensure that the stored data isn't manipulated against his/her will and likewise the SC need assurance that the stored data isn't unduely exposed. Many, if not most, of the free public file storage services do not offer data confidentiality services. Data integrity are offered to the extent that this is directly supported by the file systems used. The quality may be acceptable for most uses, but fails to cover cases where the SP is the source of the threat.

We also want access control for our data. The default should be that the SC is the only one with access. Other parties may be granted full or partial access by the SC. The service producers commonly provide schemes to allow this kind of access control. The authentication provided seems generally to rely on passwords and it seems only to be unilateral. We have not assessed the strength of the schemes, but suffice to say that they are designed for "low grade" systems. That is, they are probably fairly weak, but may still be statistically adequate for the given purpose. We therefore propose to rely on the existing authentication and access control scheme offered by the service producer, but we do not exclude the possibility of enhancing it.

Requirements (partially fulfilled):

- Identity privacy (not addressed)
- Data confidentiality (strong requirement)
- Data integrity (partially fulfilled)

- Consumer-Producer Authentication scheme
- Access control (acceptable)

To summarize, we **must** provide data confidentiality and we ought to provide data integrity services. When it comes to the scope of the protection it should be evident that file data must be protected, but there is also a strong case for protecting file system data, particularly the file/directory names. One may provide enhanced access control, but there will be a cost to doing this. One also improve the authentication, but it may be the case that the access oriented authentication is sufficient when one consider a scheme in which the data is explicitly protected independently of the access procedures. The two last requirements above will therefore largely be for the existence of an adequate solution.

2.2.3 Trust Aspects of the Consumer-producer Relationship

The legal/contractual relationship is defined by the ToS, but what about the trust aspects? There are ways of assessing trust in an online context. We approaches such as the one laid out in (Pelechrinis et al., 2011) with automated evaluation of Q&A sessions over so-called online social networks (OSN). Reputation is keyword here and there are formalized approaches that directly uses reputation in the model (Jøsang, 2010). A survey of relevant proposals for handling trust and reputation in an online context is found in (Jøsang et al., 2007). Of course there are many aspects to trust. In (Køien, 2011) the author discusses this in the context of publicly available IoT services, and while the cloud context is somewhat different from an IoT context, many of the same ideas of trust in an IoT environment will also apply to cloud services. This leads us to assume that trust in free public cloud based services will largely be based on reputation and association with well-known brands. This is not the soundest basis one can have for security, and so we must provide some means of enforcement for the trust be warranted. Another survey paper handling trust and trust management in an internet application context is found in (Grandison and Sloman, 2000). The context is not specific to cloud services, but the discussion is relevant in that it handles trust and decision making for internet applications.

2.2.4 Control Aspects of the Consumer-producer Relationship

Who has control in our Consumer-Producer relationship? Given the asymmetry in power regarding the ToS it should be clear that SP obviously has both jurisdictional control and operational control over the service. That is, the control is there as long as the consumer continues to use the service. There are several free file storage services in the market and there is therefore a certain amount of competition. The consumer may have concrete needs, but he/she can nevertheless choose between different alternatives. However, once we have actually made a choice there will be transaction costs to switch to an alternative service. We should add to this picture that many services comes in bundles and as pre-installed software on smart mobiles, tablet and laptops. So we may conclude that he consumer has a great deal of power to choose, but that the ability is impeded by imperfect knowledge, by default (pre-installed) solutions, by technical inability to change configuration and by loss of convenience and cost optimizations.

2.3 The Conflicting Incentives Approach

2.3.1 Conflicting Incentives Risk Analysis

The Conflicting Incentives Risk Analysis (CIRA) (Rajbhandari and Snekkenes, 2012) is a method for analysing risk under circumstances where it is hard to assess incident probability. This may be the case for infrequent events and generally for circumstances where past history cannot be used to predict future likelihoods. The CIRA method will instead assess the motives and incentives of the different principals. To do so the method draws on game theory, economics, psychology and decision theory. When analysing the ToS threat scenarios we may benefit from using a similar approach. Technical threats by external intruders are of course still a major concern, but what if the motives and incentives of the principals are themselves a main driver behind many of the threats?

2.3.2 The Utility Function and the Strategy Concept

In CIRA one has defined a risk owner and it defines the perspective taken. To our end we define the SC as the risk owner. The SP is the other principal entity. Then we have the strategy concept. A strategy is here some action that is intended to influence the utility function. The strategy owner is the principal that is in a position to execute the strategy. In our case we want to define strategies that lower the threat against stored content and the utility function must correspond to these goals. That is, the utility function must capture the requirements in section 2.2.2. Any strategy that positively contribute to this end is seen as desirable. There will be transaction costs to executing a strategy and it is thus not obvious that one should always execute a strategy, but even the awareness of an available strategy may be beneficial.

2.3.3 Mindset

We don't specifically propose to apply the CIRA method as as such, but we do advocate to have a "Conflicting Incentives" mindset when analysing ToS threats. That is, to keep in mind that the other principal party will have different interests and that those will govern it's actions. The consumer had better account for this and carry out actions (strategies) to mitigate or prevent negative outcomes. The key to success is to identify the appropriate utility function(s) and to identify useful strategies that address dire threats and unacceptable risks.

2.3.4 Content Ownership

A prudent question in all security is "What are the assets?" In our context the parties will be the SP and the SC and clearly the stored "contents" is an asset. Content ownership, copyrights etc. are potential "conflicting incentives" areas. SC must therefore assume that he/she must contribute something to SP in the deal. One obvious contribution is information and another is potential future loyalty. Of course, actual "contents" may also be contributed. This can be a win-win situation, like a consumer uploading content to YouTube - where both parties win if the content is widely shared.

The content in our case is exclusively provided by the user (SC), but may be used or licence by the SP (depending on ToS conditions). While there may be win-win situations we also have the distinct possibility that the equation is unbalanced and that it can even be a negative sum game (Burgess and Burgess, 1997). The utility function may be hard to define, but in a game theoretical sense we can only assume that the function is such that at least one part will expect a positive outcome (Binmore, 2007).

The "expect a positive outcome" part highlights the fact that there is a distinct difference between real and perceived utility. We shall not go into the psychology of perception here, but suffice to say that emotional responses is important. In (Camerer, 2011) one discusses how emotions and limited foresight affects our perception of utility and ultimately our decision making.

3 TERMS-OF-SERVICE POLICY CONTROL OPTIONS

ToS policies of most cloud service providers are presented in the form of long text in plain English that most users will never read. However, reading and understanding of such policies are crucial for security and privacy for users of these services. Since such policies may be a subject to change, the continuous monitoring of security and privacy related changes is necessary and could be implemented as a part of MaaS (Monitoring-as-a-Service) (Meng and Liu, 2012). One possible approach can be based on text analysis and meaning extraction with special focus on those parts of ToS policies that can potentially influence users security and privacy. By timely identifying such threats, users could undertake necessary measures to protect of both their security and privacy as required by their own policy. Possible measures could be, for example, to enforce encryption of downloaded content to guaranty confidentiality; to enforce encryption or anonymization of some parts of the content to provide privacy; to require distribution of data among several independent service providers to increase availability, etc. It is important for users to be aware of treats that potentially may appear as result changes in ToS policies. In that, there is a need for formal representation of policies, for example in P3P style, to simplify extraction of features that can be a security and privacy threats for the users. However, since ToS policies are usually written in plain English we have to deal with natural language understanding. Since it is generally a difficult problem one cannot expect a perfect solution. Our approach is to propose a practical approach that will help users to monitor changes of ToS but, in the end, will need human involvement to make final decision.

One notable feature of many ToSs is that many of them permit the service provider to *a)* unilaterally change the ToS and *b)* to only inform the service user by notification on a webpage and possible by an email. Thus, even the interested consumer may not notice that there has been a change in the ToS. Even uninterpreted notification by the policy monitoring agent (PoMA) will therefore have value.

3.1 Case Study

Let us consider some example of ToS policies of some well-known companies. Such policies are presented in plain English and therefore a method for text analysis and meaning extraction should be developed. To illustrate our idea we have extracted sentences containing keywords *grant*, *right to use*, *license to use* or *to distribute* in ToS policies of some popular cloud service providers:

- From Linkedin: “ . . . you grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free **right to** us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, **use** and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including, but not limited to, any user generated content, ideas, concepts, techniques or data to the services, you submit to LinkedIn, without any further consent, notice and/or compensation to you or to any third parties . . . “
- From Instagram: “ . . . you hereby **grant** to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide **license to use** the Content that you post on or through the Service, subject to the Service’s Privacy Policy,. . . “
- From Evernote: “ . . . you **grant** Evernote a **license to** display, perform and **distribute** your Content and to modify (for technical purposes, e.g., making sure content is viewable on smart phones as well as computers) and reproduce such Content to enable Evernote to operate the Service. “
- From Facebook: “ . . . you **grant** us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license **to use** any IP content that you post on or in connection with Facebook (IP License). “
- From Box: “ You hereby **grant** Box and its contractors the right, **to use**, modify, adapt, reproduce, **distribute**, display and disclose Content posted on the Service solely to the extent necessary to provide the Service or as otherwise permitted by these Terms. “
- From Comcast (and Plaxo): “ If you post any content to the Comcast Web Services, you hereby **grant** Comcast and its licensees a worldwide, royalty-free, non-exclusive right and **license to use**, reproduce, publicly display, publicly perform, modify, sublicense, and **distribute** the content, on or in connection with the Comcast Web Services or the promotion of the Comcast Web Services, and incorporate it in other works, in whole or in part, in any manner. “
- From Amazon: “ . . . you **grant** Amazon a nonexclusive, royalty-free, perpetual, irrevocable, and fully sublicensable **right to use**, reproduce, modify, adapt, publish, translate, create derivative works from, **distribute**, and display such content throughout the world in any media. “

The list of keywords can be easily expanded and patterns for matching can be regular expression for example such as: {grant | license | right} to <company_ name> or {license to {use | reproduce | modify |distribute }.

Just reading these few extracts provide users with hints of potential threats to their security and privacy from these services, that is an understanding that service providers keep the right to use, distribute etc. their content.

3.2 Monitoring Terms-of-Service Policies

In order to be aware of possible security and privacy treats users have to be aware of changes in ToS policies. Monitoring and detection of changes should support two features: discovering of changes in ToS policies and discovering of security and privacy related changes in ToS policies. The first kind of changes is easy to implement, since it means detection of any changes in a text and does not require understanding of these changes. The second feature requires at least a rudimentary understanding of texts.

Some cloud-monitoring applications have already been described in the literature, for example, SLA Violation Detection (Emeakaroha et al., July), Resource Usage (Dhingra et al., 2012), etc. However, we could not find any policy monitoring applications.

In our approach, we propose to use monitoring agent running locally on users computer and analyzing changes of ToS policy each time user use the service. The user register websites policy locations in the agent database for each cloud service he/she uses. Monitoring agent analyzes the policy text to detect changes from last time the service was used. The monitoring is based on the idea informally presented in the previous subsection. In case the change is detected, the agent will identify new sentences, removed sentences and modified sentences. By matching patterns, the agent extracts sentences (containing patterns) that may be potentially associated with security and privacy threats.

For example, pattern license to {use | reproduce | modify | sublicense |distribute} means that confidentiality of users data may be violated. If it is a storage service and such feature is considered as violation of users security policy an encryption of all data have to be activated. An example of configuration table for the PoMA is shown at Figure 1.

ToS location	Pattern	Violation	Action
http://instagram.com/ about/legal/terms/	{grant|license|right} to {use|reproduce|modify |sublicense|distribute}	Privacy	Encryption
https://www.box.com/	-"''-	Confidentiality, Privacy	Encryption
http://www.linkedin.com/static? key=user_agreement& trk=hb_ft_userag	-"''-	Privacy	No actions available

Figure 1: Configuration table for ToS monitoring agent.

4 CLOUD BASED STORAGE SERVICES

4.1 File Storage and Synchronization Services

There are several publicly available cloud-based file storage services like Dropbox, Google Drive and Microsoft SkyDrive. Generally, the free services are restricted in the amount of storage they offer. These file storage services mirrors a directory tree at the target computer. All files placed in the target directory will be synchronized and a copy of the files will be stored in the cloud by the service. The beauty the schemes is that one may synchronize several computers this way.

Enterprises and businesses are understandably concerned about storing their essential business data in a public cloud storage facility. In the article "New Approaches to Security and Availability for Cloud Data" (Juels and Oprea, 2013) the authors discusses these problems and proposes some solutions. The tenants (consumers, SC) will have to be convinced that security and availability is ensured or otherwise they will tend to favour private clouds instead of public clouds. The power balance between a paying tenant (SC) and a public cloud service provider (SP) may not be balanced, but SP clearly have an incentive to accommodate the paying tenant. Our perspective is a little different from that of (Juels and Oprea, 2013) our scope for cases where the power balance is very different. We also assume a model where the data is mirrored at the tenants computers. Free services will also have some kind of authentication and access control, but that is very often all that is provided. Use of cryptography is clearly necessary to provide credible security for data stored in a public cloud and availability may dictate schemes similar to the RAID inspired HAIL scheme proposed in (Juels and Oprea, 2013). HAIL itself is an acronym for High-Availability and Integrity Layer (Bowers et al., 2009). We do not consider a HAIL-based approach here. Instead, we do propose a model with basic security services implemented at the presentation layer. Our scheme is in concordance with Presentation layer in the Systems Interconnection (OSI) Reference Model, and this also means that the implementation is at the host (tenant) and not at the SP.

4.2 An OSI "Presentation Layer" Solution

The OSI reference model (ISO/IEC 7498-1, 1994) is defined by the International Organization for Standardization (ISO). The OSI RM is a way to describe and characterize a communications stack in terms of abstraction functions defined at different layers. Each layer serves the layer above it and is served by the layer below. Layer 6 is the *presentation layer* and it is primarily concerned with services such as data representation, encryption and decryption, converting machine dependent data to machine independent data etc. For connectionless services (IP-based) recommendation (ISO/IEC 9576-1, 1995) applies.

4.3 The Umbrella Architecture

Our proposal, which we call the **Umbrella Architecture**, is depicted in figure 2. The proposal combines the services of the presentation layer security manager (PLaSM) and the policy monitoring agent (PoMA). In our scheme we have let there be a local PoMA which communicates with a MaaS cloud service to carry out the actual ToS monitoring. We optionally also propose to have a *reputation manager* in the system. The reputation manager will use methods discussed in (Jøsang, 2010; Pelechrinis et al., 2011) to extract information about the reliability and trustworthiness of the SP. The work in (Pelechrinis et al., 2011) will need to be extended to achieve full "reputation" handling. We do not further develop the reputation manager concept in this paper.

4.3.1 Scope and Basic Architecture

We do not attempt to cater for all possible security

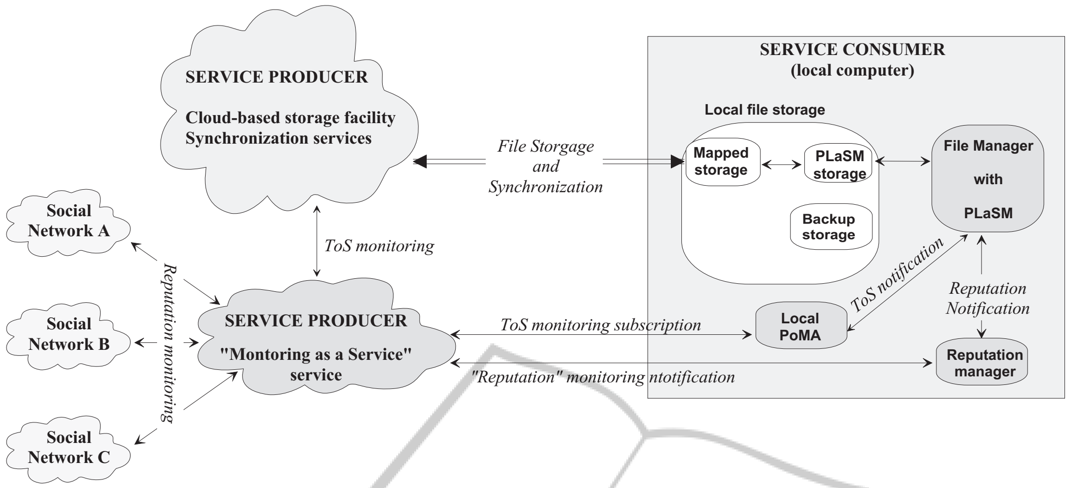

Figure 2: The Umbrella Architecture Concept.

services. Instead, we attempt to define a light-weight solution that may be implemented in web browsers and file browser as a simple plug-in service.

- Simple AAA Service
- Data Integrity service
- Data Confidentiality service

Services such as a “Time vault/Backup” and a “Cloud withdrawal” should also be considered.

4.3.2 Service Resolution

Our model is based on a basic synchronized data storage service. It is important that the new security services fit with this model. For instance, since the synchronization is file based then the security services should also be file based. Disk encryption schemes, like for instance TrueCrypt (TrueCrypt Developers Association, 2013), work by creating a huge encrypted file and then presenting this a directory or a disk volume. Such a scheme would force synchronization of the entire “disk”, which in most cases really is *not* what one would like.

Our preliminary analysis indicates that the service resolution should be “file based”. This should include meta-information such as file names, which may be sensitive, and even files sizes. Files may also be padded up to specified block lengths, where the block length could be set according to common file system block lengths. We adopt the view that filenames should be protected and that padding should be used.

4.4 The Presentation Layer Security Manager

We primarily foresee the presentation layer security manager as a plug-in service to the “normal” file manager, and it may be available in productivity software (office packages) and in web browsers. It may be inspired by tools such as the HP ProtectTools (HP, 2010) or similar.

4.4.1 Identification and Security Context Setup

One drawback to having a client-side solution is to have to manage security at the client-side. The PLaSM must authenticate **SC** and create a security context so decipher/encipher the system information and the files whenever needed. This adds complexity and its own share of security management problems, but should nevertheless be feasible. We propose that the SC identity used is the same as used for the cloud service itself. The password, or other security credential, should for obvious reasons *not* be similar to the one used to access the cloud service. As of now the choice of credentials and the actual security context is left for further study, but suffice to say that the credentials should be flexible in use and not themselves represent a security weakness.

4.4.2 Security Service Provisioning

We aim primarily at providing data confidentiality and data integrity. This should include concealment of file/directory names and file length padding. Standard file encryption methods seems adequate here. As a minimal solution for data integrity should be implemented on a per-file basis, but one may also have file system integrity built into the system. The integrity solution should not implemented such that it itself unduely increase the synchronization activity of the cloud service.

5 CONCLUSIONS

In this paper we have defined and addressed problems associated with the so-called ToS threat. The ToS threat is not exclusive to cloud services, but is highlighted by the ubiquitousness and proliferation of cloud based services. The ToS threat is mostly seen as a threat towards unpaid and publicly available services, but the threat is in principle generic.

Our Umbrella Architecture is very much work-in-progress. The concept seems sound enough, but more analysis is needed both in terms of services to be provided and the general usability of the concept. Clearly, the effectiveness and the efficiency of the approach must be investigated too. The basic PLaSM seems feasible and useful, but scalability with respect to use on multiple platforms must be investigated. The PoMA and ReMA seems in principle to be interesting and reasonable schemes, but it must be verified how useful and precise these schemes are in practice.

So we conclude optimistically that we consider the Umbrella Architecture to be an interesting and feasible approach, but that it is at a very early stage of development. Only further study can determine how practical and useful the architecture really is.

REFERENCES

Bernsmed, K., Jaatun, M., Meland, P., and Undheim, A. (2011). Security slas for federated cloud services. In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pages 202–209.

Binmore, K. (2007). *Playing for real: a text on game theory*. Oxford University Press, USA.

Bowers, K. D., Juels, A., and Oprea, A. (2009). Hail: a high-availability and integrity layer for cloud storage. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 187–198, New York, NY, USA. ACM.

Braman, S. and Roberts, S. (2003). Advantage isp: Terms of service as media law. *New media & society*, 5(3):422–448.

Burgess, H. and Burgess, G. M. (1997). *Encyclopedia of conflict resolution*. Abc-Clio Santa Bárbaraˆ eCalifornia California.

Camerer, C. F. (2011). *Behavioral game theory: Experiments in strategic interaction*. Princeton University Press.

Dhingra, M., Lakshmi, J., and Nandy, S. K. (2012). Resource usage monitoring in clouds. In *Grid Computing (GRID), 2012 ACM/IEEE 13th International Conference on*, pages 184–191.

Emeakaroha, V., Ferreto, T., Netto, M., Brandic, I., and De Rose, C. (July). Casvid: Application level monitoring for sla violation detection in clouds. In *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual*, pages 499–508.

Grandison, T. and Sloman, M. (2000). A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE*, 3(4):2–16.

HP (2010). HP ProtectTools Security Software; technical white paper.

ISO/IEC 7498-1 (1994). Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. In *ISO/IEC 7498-1:1994*. ISO, Geneva, Switzerland.

ISO/IEC 9576-1 (1995). Information technology – Open Systems Interconnection – Connectionless Presentation protocol: Protocol specification. In *ISO/IEC 7498-1:1994*. ISO, Geneva, Switzerland.

Jøsang, A. (2010). Subjective logic. *CA: University of Oslo*.

Jøsang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644.

Juels, A. and Oprea, A. (2013). New approaches to security and availability for cloud data. *Commun. ACM*, 56(2):64–73.

Køien, G. M. (2011). Reflections on trust in devices: An informal survey of human trust in an internet-of-things context. *Wireless Personal Communications*, 61:495–510.

Meng, S. and Liu, L. (2012). Enhanced monitoring-as-a-service for effective cloud management.

Oleshchuk, V. A. and Køien, G. M. (2011). Security and privacy in the cloud a long-term view. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, pages 1–5. IEEE.

Pelechrinis, K., Zadorozhny, V., and Oleshchuk, V. (2011). Automatic evaluation of information provider reliability and expertise. *SIS-2011-04-TELE-001-Technical report*.

Rajbhandari, L. and Snekkenes, E. (2012). Intended actions: Risk is conflicting incentives. In Gollmann, D. and Freiling, F., editors, *Information Security*, volume 7483 of *Lecture Notes in Computer Science*, pages 370–386. Springer Berlin Heidelberg.

Schneier, B. (2013). Terms of service as a security threat.

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1 – 11.

Thomson, I. (2012). Instagram back-pedals in face of user outrage.

TrueCrypt Developers Association (2013). Free open-source disk encryption software.

Zhao, G., Rong, C., Jaatun, M., and Sandnes, F.-E. (2010). Deployment models: Towards eliminating security concerns from cloud computing. In *High Performance Computing and Simulation (HPCS), 2010 International Conference on*, pages 189–195.