A Data-centered Usage Governance: Providing Life-long Protection to Data Exchanged in Virtual Enterprises

Jingya Yuan[a], Frédérique Biennier[b] and Nabila Benharkat[c]
University of Lyon, CNRS, INSA-Lyon, LIRIS UMR 5205, Lyon, France

Keywords: Collaborative Networked Organisation, Usage based Access Control, Distributed Usage Governance, Blockchain.

Abstract: Since the early definition of the Virtual Enterprise concept in the 90s, efficient information sharing and trust have been pointed out as major challenges to support the enactment of collaborative organisations. By now, traditional Collaborative Business support systems have been designed to interconnect corporate Business Processes and different well-known information systems, whereas trust is mostly managed thanks to inter-personal relationships. Unfortunately, this well-perimetrized vision of a Collaborative Network Organization does not fit the large scale, opened and evolving context due to the fast adoption of Industry 4.0 and sharing economy models which rely on the large scale adoption of Social Mobile Analytics Cloud Internet of Things technologies (later called SMACIT for short) and semi-opened information systems. This involves rethinking the way information, services and applications are organized, deployed, shared and protected, moving from the traditional perimetrized system protection to data and service life-long usage control. To this end, we propose a data-driven security organization which uses a multi-layer architecture to describe on one hand the logical organisation of the information system, i.e. the data assets and the business services needed to implement the collaborative business processes and on the other hand the multiple copies exchanged with different service providers. Based on this Information System meta-model, our system integrates a blockchain-based usage manager to govern the way information are exchanged and processed.

1 INTRODUCTION

Whereas Collaborative Networked Organisations (later called CNO for short) have been studied for decades since the earliest virtual enterprise definition in the 90s(Browne et al. 1995), the fast development of digital and sharing economy coupled to the wild adoption of SMACIT technologies renew these CNO models to large scale and semi-opened "on demand" CNO enactment. As pointed out in earlier studies, trust and reputation are key elements to identify potential partnerships (Baroudi et Lucas 1994), (Jøsang et al. 2007). Whereas different Business related models and criteria (such a cost, delay, product / service quality…) have been used to evaluate trust and reputation (Hendrikx et al. 2015), security and privacy related criteria must also be considered as information sharing with potential competitors can be a major threat (Panahifar et al.2018).

Protecting traditional information systems (including physical systems, processes and the information they use) relies on methods to identify precisely threats and vulnerabilities, prioritize them and mitigate the main risks by deploying adapted technical countermeasures. For example, data replication provides availability, data encryption and access control increase confidentiality level whereas hashing techniques (used to "sign" critical data value) and log registrations are used to fit integrity requirements. Nevertheless, these protection strategies are designed for a well-pereimetrised environment and well-known information system organisation whereas the semi-opened collaborative environment involved by SMACIT and sharing economy requires controlling Business Process

[a] https://orcid.org/0000-0002-9853-7118
[b] https://orcid.org/0000-0001-6908-6103
[c] https://orcid.org/0000-0002-1911-5524

Yuan, J., Biennier, F. and Benharkat, N.
A Data-centered Usage Governance: Providing Life-long Protection to Data Exchanged in Virtual Enterprises.
DOI: 10.5220/0009349501770184
In *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020) - Volume 2*, pages 177-184
ISBN: 978-989-758-423-7

(Weber et al.2018) as they can be seen as potential threats.

To define and manage consistently assets protection in opened environments, we propose a data-driven protection architecture. By integrating business usage purpose, a finer-grained contextualized protection is set. Then, we use a governance loop to collect the service real quality of protection, including the trust level associated to the service provider. This architecture allows a consistent evaluation of the current protection of assets and a finer-grained control on the real usages.

After presenting the related works, we describe our distributed data-driven protection architecture before comparing it with other works (section 4).

2 RELATED WORKS

As SMACIT and CNO integrate different actors (such as service providers, hosting platform managers…), they can be deployed world-wide, leading to integrate different legal regulations constraints. Such complex distributed organisation makes protecting (personal) data harder as different parties may exchange and share these data in a non-protected way. According to a societal point of view, this can appear as "unfair" practices but service consumers / end users have only few ways to manage their security / data privacy preferences: they can accept or refuse the security / privacy conditions of the service provider, select providers depending on a subjective trust level…

Access control has been seen as a fine-grained trust model. It may be used to restrict access to well-identified trusted users, using the simplest Access Control List to name them or Role based Access Control (RBAC) (Sandhu, R. S et al. 1996) to integrate basic organisational knowledge to identify the in a more generic way. Extra organisational knowledge described in Organizational Based Access control OrBAC (Autrel, F et al. 2008) or contextual information identified in Attribute Based Access Control (Wang et al. 2004) can be used to precise the usage context. Lastly, Usage CONtrol (UCON) (Park, J., Sandhu, R 2004) enriches the 'Attribute-based access control' model with "Rights" and "obligation" parts thanks to dedicated languages such as Obligation Specification Language (OSL) (Hilty, M et al. 2007) or Rights Expression Languages (RELs) (ISO et IEC. 2004) from the DRM area (Open Mobile Alliance 2008). Other features fitting the distributed environment challenges can also be added, such as

- Tracking data flows to enforce usage control requirements at all relevant systems layers (Pretschner et al. 2011) or for different data copies in distributed systems (Kelbert, F., et Pretschner, A 2013).
- Providing extended usage policy language to implement the server-side usage control architecture (Pretschner et al. 2006) or to integrate social networks conditions (Kumari et al. 2011).

Despite their interest, these access control features do not protect data against unpredictable and "unfair" usage such as uncontrolled copies of data stored in social networks or analytics processes extracting new data and knowledge to serve different business goals leading to privacy breaches.

To face this risk, GDPR empowers users with their personal data protection, requiring service providers to state and prove usages they have for a particular data. This involves managing user consents accordingly and reporting any security breach to the data owner. To fit these legal obligations, several works have been developed either (i) to identify both information and processing categories in traditional Enterprise Architecture models in order to simplify the data usage control (Burmeister et al.2019) or (ii) to manage data collection and tracking data flows between stakeholders (Cha, S. C., et Yeh, K. H 2018) … Focusing on the way "fair and accepted usage" can be proved, several works have focused on the blockchain immutability property: (i) to manage access control function such as (Di Francesco Maesa. et al. 2017) which uses smart contracts to embed access control rules, (ii) to manage data encryption key used to protect data access (Wirth, C., et Kolain, M. 2018), (iii) to manage user consents(Truong, N. B. et al. 2019) or (iv) to track data accountability and provenance (Choi, C et al.2014) as well as usage operation thanks to smart contracts generated according to the data usage policy (Neisse, R. et al.2017).

Despite this rich background, several challenges remain. First, data usage does not integrate business purpose. It means that policies are defined for well-identified processes, whereas the opened environment involves considering more generic risks. Second, as data protection is designed for a "stand-alone" information system, this may lead to security breaches for both data owner and data consumers when inconsistent usage are granted for the different copies dispatched in several information systems.

3 DATA-DRIVEN COLLABORATIVE USAGE CONTROL ARCHITECTURE

To provide a consistent protection for data in opened collaborative environments, we propose a data-driven protection architecture plugged on the information system thanks to a dedicated Information System Interface component. First, the protection persistency layer relies on an information system meta-model, describing the information system organisation and its interactions with its environment. This meta-model allows identifying assets logically and defining their Requirements of Protection (RoP) depending on their assets' value. These RoP are propagated to the assets' multiple copies. Second, the asset protection layer extends the traditional protection features and usage-based access control models to integrate organisational knowledge and process purpose so that Terms of Usage (ToU for short) are defined more precisely, restricting potential business usage and identifying the necessary protection features. Third, the usage governance layer relies on a blockchain-based registration of data exchange and usage to evaluate any violation of the approved ToU.

3.1 Protection Persistency Model

To support a consistent protection on the multiple copies of a logical assets, we design a multi-layer meta-model integrating:

- **The Data Collaborative Ecosystem Description**, defines (i) who (human being or organization entity) owns the data, processes it, stores it…, (ii) contracts, including Terms of Service and security agreements, between stakeholders and even (iii) trust relationships between stakeholders
- **The Logical Information System Meta-model**, includes the description of (i) the data assets and their requirements of protection depending on the data value and sensitivity and (ii) the way they are used, i.e. a description of abstract business services including their business purpose)
- **The Description of the Different Physical Copies of a Logical Data** (called later containers) and the real concrete service (IT or manual) processes acceding to these data.

Thanks to this multilayer meta-model, relationships between logical assets (data or business services) and their physical instances (copies or concrete services) are used to manage a consistent protection, propagating requirements to the "physical instances" and tracking real usage to "rebuilt" the current protection in a life-long protection vision.

3.2 Usage-based Asset Protection

Taking advantage of previous works as UCON (Park, J., et Sandhu, R. 2004) and of the service-oriented security architecture, we propose a policy ontology (see fig 1) integrating both asset sensitivity and usage to define Requirements of Protection (RoP) related to logical data and Quality of Protection (QoP) related to Business Service that will "consume" a data container.

- **The Asset Classification** defines the data visibility (private / public or restricted) depending on its sensitivity. An Explicit identifier / quasi-identifier qualification is added to fit some risks involved by the analytics / mining process in order to consider anonymization/obfuscation requirements.
- **The Usage Ontology** is used to describe the different actions. It includes classical operations such as Read, Write, Send, Receive, Execute, Delete, Modify, Track, Create. It is enriched with usages dedicated to Social media, Mobile and Analytics context, including Share/Post, Follow, Interact, Tag, Record, Log record (authentication and authorization), Collect, Preserve, Search, Transfer, Visualization, Associate, Analyse, Extract, Store, Mine (Deduce) for the Mobile, Social and Analytics part. Lastly, we also integrate business purpose description (defining "why") to provide business-based usage description.
- **The Security Mechanism Ontology** integrates security services (confidentiality, integrity, availability, non-repudiation) and security mechanisms such as cryptography, authentication protocols, secure communication protocols, filtering mechanisms (firewall…) …
- **Context Information** defines different usage-control criteria such as When (operation time and duration), From Where (refers to the machine type (personal / shared / professional), the geographical location (at home / business / given state), the access network (Mobile / wired / Wifi…), the "organisational location" (i.e. the organisation department, Marketing, Supply management, Manufacturing, Maintenance)), Why is associated to the usage objective (refers to both the generic purpose which includes business usage (statistics, treatment, analyse…) coupled with the business purpose and organisation knowledge) and Who (refers to the subject

definition (unknown, trusted group, precise actor)).

• **Security and Usage Tracking Maturity** states if and how real usage or security breaches are reported. It refers to a "report maturity" indicator: "no" means that no data is available, "logged" means that actions are stored, "managed" means that the tracking part is identified and "proved" means that the tracking part is certified and published.

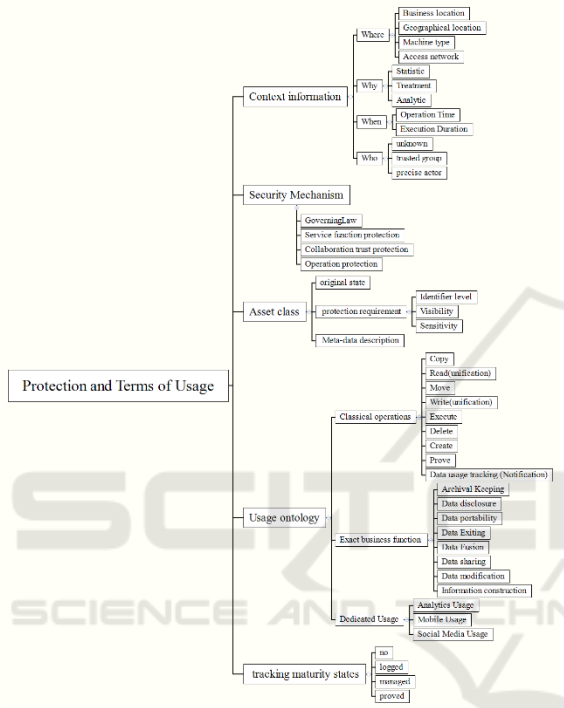

Figure 1: Policy assertion ontology.

3.3 Protection Governance

To provide the life-long asset protection, our policy assertion ontology is in charge of defining the way a data asset can be used by a business service before providing a copy of the data asset to this service and tracking the real usage of this asset copy. These requirements involve that the data driven protection architecture is distributed on both data owner and data consumer side.

Designed in a loosely coupled strategy, our system is built on a Protection Management component, managing our Information System meta-model. This component uses the Information System Interface Manager component to capture service invocation, required information identification by analysing the meta-data included in the web pages DOM…. This interface is in charge of invoking the protection management component.

The protection management component interacts with the protection persistency component, in charge of establishing our meta-model to interact with Terms of Usage management component to manage the Requirements of Protection and Terms of Service associated to logical assets and Business services. It consists in an Asset Manager, associated to the logical asset and related business services, a Service Manager, associated to logical asset and related abstract services, and in an Operation Manager in charge of physical containers and concrete services. It generates and manages physical containers storing the copy of the asset used by a given Business Service. Paying attention to the data consumer side, the origin of each container can be tracked and each container is associated to its Terms of Usage, defining the way it can be used and processed. Focusing on the Data owner side, this allows building a consistent Asset protection dashboard, aggregating the different copies' ToU, so that due and undue usage can be identified.

The Terms of Usage management component (ToU manager for short) is designed to negotiate the protection and control contracts between the data owner and data consumer (see figure 2). It is launched each time a Business Service requests a data. ToU is evaluated according to both Data Owner RoP and Data Consumer Terms of Service, including the description of usages and protection. To this end, the Security Manager starts on the data consumer side, by identifying the asset description (i.e. the associated meta-data) and the associated Terms of Service (ToS for short). The ToS is generated by aggregating sub-services QoP and ToS protection, using a lax aggregation rule (i.e. keeping the less protecting level for each protection assertion). Once this ToS policy is generated, the protection manager sends it to the Data Owner Protection Manager to evaluate this proposal as a potential Terms of Usage via the Exchange interface. On the data owner side, the Protection Manager sends it to the Asset Manager to identify the corresponding assets and their associated Requirements of Protection. Then, the Security Manager, on the Data Owner side, aggregates the requested assets RoP, using a strict aggregation rule (i.e. the more protecting and more reduced usage authorisation strategy). This consolidated RoP is then compared to the proposed Usage management protection policy and a ToU restricting the initial protection to RoP conditions is set. Of course, if the proposed protection does not fit the aggregated RoP, the Data Owner can be notified and may decide to

modify the RoP accordingly. Then the Data Owner signs this ToU and sends it for approval to the Data Consumer Usage manager. This negotiation phase is concluded when the Data Owner Usage Manager generates the exchange smart contract (see figure 3) allowing authenticating both Data Owner (to certify the container origin) and Data Consumer while managing the container encryption accordingly. A token associated to the approved ToU is stored in the Blockchain to prove the consent.

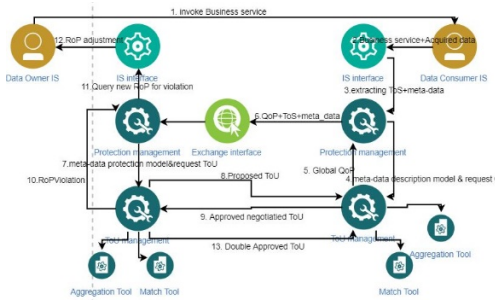

Figure 2: ToU negotiation process.

```
pragma solidity ^0.4.21;
contract ExchangeSmartContract{
    string constant identification_prove='I am the data consumer';
    string constant Terms_of_usage_Token='xxxx';
    event Transfer(address indexed _from, address indexed _to, string _terms_of_usage_ID);
    string constant terms_of_usage_ID='isliss';
    string constant KeyDataconsumer='xxxxxx';
    string constant owner='xxx';
    uint256 constant key='xxxx' ;// the data consumer's public key
    function authenticate(string para)public returns(bool){
        if(identification_prove==decrypt(para))//decrypt the string to identify the msg.sender's identity
        return true;
        else
        return false;
    }
    function acquiration(string para)public returns(string){
        //only the data consumer can acquire the token
        require (authenticate(para)==true);
        emit Transfer (owner, msg.sender, terms_of_usage_ID);
        // send the notification to data owner to start the tracking agent
        return(Terms_of_usage_Token);
        //give data consumer the token
    }
    function decrypt(String para) public returns(String){
        .....
    }
}
```

Figure 3: Exchange smart contract.

If the ToU mentioned that usage will be at least reported, the Usage monitoring process is launched on the Data Owner side as soon as the exchange smart contract is invoked (see figure 4). To this end, the Usage Monitoring component notifies the Global Tracking Agent on the Data Consumer side that it will follow operations on the container. In a symmetric way, on the Data consumer side, once the exchange smart contract is invoked, its Usage manager generates Usage smart contracts (see figure 5) monitoring by the Complex tracking agent. Similarly, the Operation manager, in charge of the logical access operations on containers, generates physical smart contracts (see figure 6), coupling the physical operation on the container to an event, registering it on a log file and a tracking smart contract is generated to implement the on-line log file elementary actions tracking (see figure 7). By this way, elementary tracking agents report basic operations on the data container to the Complex Tracking Agent that consolidates them according to the precise negotiated usage, so that the Global Tracking Agent generates a global report including logfile tokens associated to usage operations for the Data Owner.

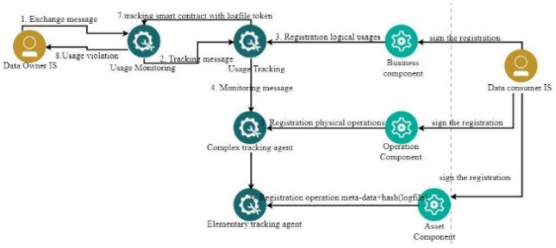

Figure 4: Usage monitoring process.

```
contract UsageSmartcontract{
    string constant identification_prove='I am data consumer';
    string constant usageID='data_portability';
    // this record refers to the Terms of Usage and represents the logical usage that data consumer will implement
    event UsageImplement(address indexed _from, address indexed _to, string usageID);
    struct PhysicalSCaddress{
        address physicaladdress;
        //the address of each physical smart contract
        string physicalname;
        //the name of each physical smart contract
    }
    PhysicalSCaddress[] public physicaladdr;
    //establish the instance of physicalSmartcontractaddress collection
    constructor (address[] addr,string[] name){
        //record all related phyiscal smart contract addresses in the UsageSmartcontract
            for(uint i=0;i<addr.length;i++){
                PhysicalSCaddress memory tmp= PhysicalSCaddress({physicaladdress:addr[i], physicalname:name[i]});
                physicaladdr.push(tmp);
            }
        }
    function usagetrack(string para)public {
        require (authenticate(para)==true);
        emit UsageImplement (owner, msg.sender, usageID);
```

Figure 5: Usage smart contract.

```
pragma solidity ^0.4.21;
contract PhysicalSmartcontract{
    //manage the physical operation and generate logfile
    event implement(address from, string to, string operation);
    function setLogfile(string _logfileID, string operation)public{
        emit implement(msg.sender,_logfileID, operation);
//the address of data container will generate the logfileID for the physical operation
    }
    ....
}
```

Figure 6: Physical smart contract.

```
pragma solidity ^0.4.21;
contract TrackingSmartContract{
    string constant implemetation='It starts to record';
    event Implementation(address indexed _from, address indexed _to, string constant implemetation);
    string usage_token;//the content of usage_token
    string _logfile_token;
    address dataconsumer;
    function ConsumerInvoke(string str1,address name)public{
        //this is invoked by the data consumer part to store the logfile_token
        require(msg.sender==dataconsumer);
        emit Implementation(msg.sender, name, implemetation);
        //notify the data owner that data consumer has implemented the physical operation
        _logfile_token=str1;
    }
    function OwnerInvoke(string memory paired_Usage_Token_hash)public returns(string){
        // this is invoked by the data owner part to get the logfile_token
        paired_usage_Token=decrypt(paired_Usage_Token_hash)
        //decrpyt the paired_Usage_Token_hash by data owner's public key
        require(paired_Usage_Token==usage_token);
        //check the msg.sender's identity and require it is the data owner
        return (_logfile_token);
    }
    ...
}
```

Figure 7: Tracking smart contract.

4 EVALUATION

To evaluate our distributed data driven protection architecture, we use a simple use case to compare our system with the existing works. OnlineShopping is a market place selling different products. Its main business purpose is product exhibition and sales with Social interaction usage. Its collaborative ecosystem integrates different parties:

- Company A is a manufacturer that uses Online-shopping to propose spare parts for its after-sales service as well as a customized "printable" product design service. Its main business purpose is product manufacturing with Cloud Computing SaaS My3Dprinter operation usage.
- Different companies such as Company B owning one of the My3D printers offer a certified "product printing service and delivery", allowing to produce the requested part from a product "ready to print" file as close as possible to the client to improve the delivery process. Its main business purpose is semi-product manufacturing and delivery with Cloud Computing SaaS operation usage and delivery feedback with Mobile visualization usage.
- MyPayment company provides a secure payment and fund transfer service. Its main business purpose is payment transaction with Cloud Computing PaaS operation usage.
- MyAnalytic company provides analysis for marketing services based on its recommendation engine. Its main business purpose is activity-based profiling thanks to mining service.

Terms of Service policies are associated to the different business services provided by the parties: OnlineShopping collects browsing activity traces and exchanges them with MyAnalytics to get adapted recommendations for its clients. It also exchanges payment information (amount and refunding company Id) and tokens with MyPayment company. Regarding the ordering service, product information and client delivery information are exchanged with its manufacturing partners.

Alice uses the OnlineShopping application which will generate different transactions with many suppliers using our system or not. First, Alice browses the marketplace and buys product X by interacting with OnlineShopping to exchange information such as name, delivery address, payment related information etc.

Alice uses our system and sets her requirements of protection to the data required by OnlineShopping:

- Web browsing activity: sensitivity level: medium, should be kept less than 30 days. This means that Alice accepts that this activity serves for undefined business purpose but the deletion should be tracked to show that the storing delay is respected.
- Personal Information with explicit identification (i.e. name, phone number) and quasi-explicit identification is highly sensitive. It should be kept and processes only for ordering and delivery purpose. This means that access should be reduced to actors and services in charge of processing the product order and product delivery, regarding Alice's address and that payment information should be kept to fit legal constraints.

Based on these requirements, we first evaluate our Terms of Usage ontology by comparing it with others. To this end, we identify 3 main comparison criteria:

- subject attribute defines the attributes of the party requiring the access,
- control objective defines the attributes which are used to describe 'Rights', 'Obligation' and 'Condition'.
- countermeasure scope includes infrastructure security, communication security, data storage and access control,

As far as the subject attribute is concerned, (Hu, Y. J et al.2008), (Nejdl et al. 2005), (Liu, C. L 2014), (Garcia et al. 2005) define generic roles. This can fit partly Alice's needs as they can be used to identify actors belonging to the convenient organisation department but they do not integrate usage-related role (such as data owner, data consumer), making harder the definition of who can be authorized to share Alice's data with Company A. Although (Chaari et al. 2008) extends these criteria to reputation and (Tsai et Shao 2011) integrates social relationships, they only allow managing (trusted) links between actors. Our ToU ontology extends the subject description to manage both individual and organizational entities. It also couples with usage-related roles and real subject identity. By this way, it can be used to identify exactly the actors allowed to decide to share Alice's address with company A, integrating business knowledge from the ordering process.

Focusing on the control objective, (Choi, C et al.2014), (Liu, C. L 2014) and (Garcia, D.et al.2009) consider either the service or the trust level associated to the stakeholder the asset while (Masoumzadeh, A., et Joshi, J. 2010), (Kim, A et al. 2005) and (Wang, L et al. 2004) propose rules associated to the semantic value of the asset. These ontologies do not support a synthetic definition of the business context, making harder to restrict data usage according to business purpose (in our example, Alice's address can be used for ordering and delivery processes). Our ToU ontology designed according to our multi-layer model extends the control object to define precisely contextual usage information associated to logical data and physical copies, including archival keeping, data portability, data sharing, CRUD operations…. This allows propagating the "restricted to delivery

purpose" usage condition on the address when a copy of it is shared with company A.

Focusing on countermeasure scope, (Nejdl et al. 2005) et al. 2005) and (Tsai, W. T., et Shao, Q. 2011) focuses on access control whereas (Kim, A et al. 2005) even integrates infrastructure condition with access control, allowing integrating the secured exchange channel constraint. Our ToU ontology integrates infrastructure, communication, data-protection and access control means by extending access control and operational service to "business purpose", i.e. generic operations fitting a business goal and "collaboration operations". By this way, the deletion constraints can be taken into account as other protection means (storing encrypted payment token, exchanging data through SSL-based channels…).

Compared to other ontologies, our ToU integrates all the necessary elements to describe usage and protection features, including data sharing and usage delegation. By this way, constraints on life-long usage control and protection features can be described using a single ontology. Moreover, the usage-related roles allow integrating the collaborative context (i.e. the relationships between stakeholders) in the fine-grained policy rules.

Then, we evaluate our Life-long Data Centric Protection system (LDCP) with other works integrating GDPR requirements, such as consent management, usage scope definition, operation tracking and life-long protection.

First, we identify that only (Burmeister et al. 2019) integrates the usage scope, i.e. business purpose. (Kaaniche, N., et Laurent, M 2017) and (Wirth, C., et Kolain, M. 2018) refer to traditional consent management which doesn't consider usage scope and is only managed by the subject. (Truong, N. B et al. 2019) retrieves the consent "signature" from a blockchain. (Neisse, R et al. 2017) and (Di Francesco Maesa, D et al. 2017) do not integrate data origin to manage consent forwarding. Our system not only manages stand-alone consents, it also integrates consents provided in a collaborative context (i.e. when information is shared by different parties). Our Usage Governance architecture, allows monitoring and evaluating the real operations on the containers, paying attention to the business purpose. Based on the different assertions, our system stores the approved ToU in a Blockchain, proving Alice's consent shared with Online Shopping as well as the approved ToU related to data sharing between Online Shopping and company A. By this way, the consent origin can be tracked. Moreover, the exchange smart contract allows certifying the data origin on the data consumer side.

Focusing on tracking abilities, (Wirth, C., et Kolain, M. 2018) controls data encryption keys to track data access and usage whereas (Neisse, R et al. 2017) tracks data forwarding and (Di Francesco Maesa, D et al. 2017) tracks right transfer. Thanks to our governance architecture, our system tracks real operations on containers (i.e. copies of the logical data) thanks to its "double approved" monitoring agents and their associated smart contracts. As our system manages the rights delegation, the monitoring feature is also extended to other stakeholders getting a copy of a data. By this way, our system controls both data usage operation achieved by Online Shopping, Company A and Company B as secondary tracking agents are generated once the data is shared. By this way, the life-long usage-based protection can be tracked and each party can prove that it has fulfilled its obligations.

5 CONCLUSION

In this paper we present a distributed usage governance architecture, relying on an information system meta-model and on Blockchain-based Terms of Service negotiation and usage tracking.

To this end, we have extended usage and security ontologies to define data protection requirements and potential usages as precisely as possible. Further works will focus on the way Information System interface components can be implemented more efficiently.

REFERENCES

Autrel, F., Cuppens, F., Cuppens-Boulahia, N., & Coma, C. (2008). MotOrBAC 2: a security policy tool. In *3rd Conference on Security in Network Architectures and Information Systems, 273-288*.

Baroudi, J., & Lucas Jr, H. C. (1994). The role of information technology in organization design. *Journal of Management Information Systems, 10(4), 9-23*.

Browne, J., Sackett, P. J., & Wortmann, J. C. (1995). Future manufacturing systems—towards the extended enterprise. *Computers in industry, 25(3), 235-254*.

Burmeister, F., Drews, P., & Schirmer, I. (2019). A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Cha, S. C., & Yeh, K. H. (2018). A data-driven security risk assessment scheme for personal data protection. *IEEE Access, 50510-50517*.

Chaari, S., Badr, Y., & Biennier, F. (2008). Enhancing web service selection by QoS-based ontology and WS-policy. In *Proceedings of the 2008 ACM symposium on Applied computing, 2426-2431*.

Choi, C., Choi, J., & Kim, P. (2014). Ontology-based access control model for security policy reasoning in cloud computing. *The Journal of Supercomputing, 67(3), 711-722*.

Di Francesco Maesa, D., Mori, P., & Ricci, L. (2017). Distributed access control through blockchain technology,31-32.

Garcia, D., Toledo, M. B. F., Capretz, M. A., Allison, D. S., Blair, G. S., Grace, P., & Flores, C. (2009). Towards a base ontology for privacy protection in service-oriented architecture. In *2009 IEEE International Conference on Service-Oriented Computing and Applications (SOCA),1-8*.

Hendrikx, F., Bubendorfer, K., & Chard, R. (2015). Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing, 75, 184-197*.

Hilty, M., Pretschner, A., Basin, D., Schaefer, C., & Walter, T. (2007). A policy language for distributed usage control. In *European Symposium on Research in Computer Security, 531-546*.

Hu, Y. J., Guo, H. Y., & Lin, G. D. (2008). Semantic enforcement of privacy protection policies via the combination of ontologies and rules. In *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 400-407*.

ISO, IEC. (2004). information technology–multimedia framework (MPEG-21) Part 5: Rights Expression Language. *International Organization for standardization*.

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

Kaaniche, N., & Laurent, M. (2017). A blockchain-based data usage auditing architecture with enhanced privacy and availability. In *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), 1-5*.

Kelbert, F., & Pretschner, A. (2013). Data usage control enforcement in distributed systems. In *Proceedings of the third ACM conference on Data and application security and privacy, 71-82*.

Kim, A., Luo, J., & Kang, M. (2005). Security ontology for annotating resources. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems",1483-1499*.

Kumari, P., Pretschner, A., Peschla, J., & Kuhn, J. M. (2011). Distributed data usage control for web applications: a social network implementation. In *Proceedings of the first ACM conference on Data and application security and privacy,85-96*.

Liu, C. L. (2014). Cloud service access control system based on ontologies. *Advances in Engineering Software, 69, 26-36*.

Masoumzadeh, A., & Joshi, J. (2010). Osnac: An ontology-based access control model for social networking systems. In *2010 IEEE Second International Conference on Social Computing, 751-759*.

Neisse, R., Steri, G., & Nai-Fovino, I. (2017). A blockchain-based approach for data accountability and provenance tracking. In *Proceedings of the 12th International Conference on Availability, Reliability and Security 1-10*.

Nejdl, W., Olmedilla, D., Winslett, M., & Zhang, C. C. (2005). Ontology-based policy specification and management. In *European Semantic Web Conference, 290-302*.

Open Mobile Alliance. (2008.) DRM Rights Expression Language V2.1. http://www.openmobilealliance.org/release/DRM/V2_1-20080805-C/OMA-TS-DRM_REL-V2_120080805-C.pdf,1-68.

Panahifar, F., Byrne, P. J., Salam, M. A., & Heavey, C. (2018). Supply chain collaboration and firm's performance. *Journal of Enterprise Information Management, 31(3), 358-379*.

Park, J., & Sandhu, R. (2004). The UCONABC usage control model. *ACM Transactions on Information and System Security, 7(1), 128-174*.

Pretschner, A., Hilty, M., & Basin, D. (2006). Distributed usage control. *Communications of the ACM, 49(9), 39-44*.

Pretschner, A., Lovat, E., & Büchler, M. (2011). Representation-independent data usage control. In *Data Privacy Management and Autonomous Spontaneus Security,122-140*.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29(2), 38-47*.

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). GDPR-compliant personal data management: A blockchain-based solution. *arXiv preprint arXiv:1904.03038*.

Tsai, W. T., & Shao, Q. (2011). Role-based access-control using reference ontology in clouds. In *2011 Tenth International Symposium on Autonomous Decentralized Systems, 121-128*.

Wang, L., Wijesekera, D., & Jajodia, S. (2004). A logic-based framework for attribute-based access control. In *Proceedings of the 2004 ACM workshop on Formal methods in security engineering 45-55*.

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. In *International Conference on Business Process Management 329-347*.

Wirth, C., & Kolain, M. (2018). Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. In *Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*.

Zhang, X., Park, J., Parisi-Presicce, F., & Sandhu, R. (2004). A logical specification for usage control. In *Proceedings of the ninth ACM symposium on Access control models and technologies, 1-10*.