Data Protection, Security and Privacy in the new wave of Cloud Computing

A Service Catalogue

A Cluster of European Research & Innovation Projects on the Cloud

A proxy solution for the storage and processing of data outsourced to the cloud.
www.clarussecure.eu

A practical approach to the cloud with legal guides and dedicated tools for SMEs and IT teams in public organisations.
www.cloudwatchhub.eu

End-to-end security and improved privacy in cloud identity management services for managing secure access control.
credential.eu

Effective and deployable solutions allowing data owners to maintain control over their data when relying on Cloud Providers for data management.
www.escudo-cloud.euv

Ensuring security in all multi-cloud environments; Agile and DevOps security.
www.musa-project.eu

A platform offering comprehensive user privacy enforcement with Privacy Authority Online Service.
www.operando.eu

Novel cryptographic concepts and methods to practical applica tion to improve the security and privacy of cloud based services.
prismacloud.eu

Holistic Data Privacy and Security by Design Platform-as-a Service Framework.
www.paasword.eu

Enabling the development and execution of time critical applications in Clouds.
www.switchproject.eu

Improving cloud security for interactive, latency-sensitive applications by seamlessly integrating security extensions of COTS CPUs.
www.serecaproject.eu

Addressing confidentiality, integrity and availability of cloud applications by means of security extensions of commodity CPUs.
www.securecloudproject.eu

Data Protection Security and Privacy Cluster in the new wave of cloud computing

The Digital Single Market (DSM) in Europe is an unprecedented opportunity to create one of the biggest digital marketplaces in the world. Cloud, the Internet of Things, 5G and big data are the building blocks for the marketplace helping to create innovation hubs where Europe's 23 million SMEs can thrive and grow.

In the era of digitalisation and in a hyper-connected global economy, cloud computing is an enabler in many industry sectors, from retail and smart manufacturing to smart agriculture and digital health. Cloud gives life-breathing properties to the many companies with no in-house IT administrator or skills to set up and manage servers and software, allowing them to scale up as their business grows. For medium-sized firms migration of new applications to the cloud can benefit from rapid upgrade cycles and low capital costs.

The challenge for Europe is to ensure it retains its leadership position in research and innovation by enabling a new wave of cloud computing fit for mission-critical applications and based on security-by-design approaches. New capabilities and greater attention to data protection and privacy not only mean more business innovation as more organisations process and store sensitive data on the cloud, but also ensure compliance with new EU regulations.

What's more, digital trade is crucial for nearly all firms, from large multinationals to small businesses, that rely on online platforms to connect and trade with customers around the world. This makes trust instrumental for a safe and reliable free flow of data (whether personal data or not).

A lot of innovation coming from the European Union's Horizon 2020 programme and specifically through the Cluster on Data Protection, Security and Privacy, which is also addressing the challenges around the free flow of data within the Digital Single Market. This includes bringing to market reliable technologies and legal instruments which are necessary for allowing cloud service providers and their users (e.g., undertakings, public authorities, natural persons) to transfer data in the cloud environment.

The services and solutions presented in this document are the results from the cluster, as we welcome a new wave of cloud computing with a greater shift towards migrating complex applications to the cloud and a growing number of multi-cloud environments.

Encryption, security management of multi-cloud applications, compliance to privacy regulations, secure data storage are all areas addressed by these projects, which target stakeholders across the European market such as small businesses, large enterprise, public authorities and government.

Turn the pages to discover more

CLARUS

Project acronym & name

CLARUS – User centred privacy and security in the cloud

- www.clarussecure.eu

CLARUS brings innovation in security-enabling techniques, attack-tolerant systems and in new architectures for secure delivery in the cloud. Its Privacy-preserving mechanisms support data anonymization, data coarsening and splitting, data encryption and searchable encryption.

The CLARUS security-by-design approach unleashes new market opportunities by making cloud services more transparent, standardised, auditable and controllable.

Who is the service/solution designed for?

Information security professionals, and especially security managers can implement privacy-by-design, which ensures users of cloud services are in the driving seat when it comes to controlling their data, such as healthcare IT teams and geospatial communities.

Open source developers, tech integrators and cloud service providers can support the CLARUS proxy solution and potentially new, secure-by-design services to their customers as the market moves closer towards security-as-a-service. CLARUS can play a key role in not only moving critical applications to the cloud but also in enabling migration from a private cloud service to a pubic one, thus increasing business benefits.

What problem is the solution/service trying to solve for your company or customers?

Most security mechanisms are commonly located within the cloud platform. This makes the cloud an impractical solution for those customers whose data is considered sensitive or mission-critical, as well as for organisations that need to comply with specific regulations on data handling.

Cloud customers also need to be assured that no intruder (within or outside an organisation) can hack the cloud and/or impersonate them, and that no denial of service will occur.

With CLARUS, cloud customers no longer need “blind trust” in their cloud service provider(s) when outsourcing their data to the cloud.

CLARUS enhances trust in cloud services through its secure and attack tolerant

framework for the storing and processing of data outsourced to the cloud. This allows end users to monitor, audit and control the stored data without impairing the functionality (including the functionality provided by high-level services such as data storage, management, retrieval, transformation, etc.) and cost-saving benefits of cloud services.

The attack-tolerant framework is based on a variety of security mechanisms controlled by cloud users without imparting functionalities provided by high-level services, such as data storage, management, retrieval, transformation, etc.) and without reducing the benefits associated with clouds, such as cost savings and ubiquitous access.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

CLARUS benefits are clearly demonstrated for geospatial data and digital health and can be extended to other uses with tight security, privacy and regulatory requirements.

Hospital IT teams can move to the cloud safely knowing that sensitive data is secure and compliant with legal regulations. Public and private organisations operating with geodata can be confident of secure data publication and processing without compromising privacy and control over data.

CLARUS also supports the free flow of data as a necessary pre-condition for attracting data business under Digital Single Market Action #14, where the removal of data localisation restrictions is expected to boost cloud service development and uptake with significant economic benefits.

CLARUS helps break down barriers to sharing digital spatial data by offering a high degree of legal and technical interoperability. By facilitating access to geospatial information for re-use, CLARUS will also contribute to the goals of the INSPIRE Directive in terms of addressing legal aspects of data sharing and technical access and interoperability issues for web-based services and spatial data interoperability.

CLOUDWATCH

Project acronym & name

CloudWATCH2 - Think Cloud Service for Government, Business & Research

- www.cloudwatchhub.eu

The CloudWatchHUB.eu is *the* place to go for educational guides and practical tools for the cloud – it's a great place to start for SMEs, schools and small IT teams in public administration.

CloudWatchHUB.eu is also the only place with direct access to cutting-edge software services and cloud solutions which are free and available for end-users. Open source is the operative word.

Who is the service/solution designed for?

Cloud computing is the great leveller offering game-changing capabilities and cost savings for Governments, public administrations, businesses and research. CloudWATCH2 targets these communities to help them make informed decisions when moving to the cloud or taking services to the market, guiding them through the different phases and offering invaluable tips on legal aspects.

What problem is the solution/service trying to solve for your company or customers?

The future of the European cloud market is directly influenced by our target stakeholders.

Millions of consumers and businesses across Europe depend on cloud computing infrastructure, perhaps critically so, to access digital services ranging from email to e-government and digital health. Creating a Digital Single Market comprising such a diverse range of digital services underpinned by cloud computing infrastructure, requires a deliberated approach to open source and open standards that enables prospective customers to compare service capabilities and pricing in a transparent way. This is where CloudWatchHUB.eu makes a real difference.

Through our Cloud Market Roadmap, we address what a healthy cloud market should look like in order to drive uptake across a very broad set of customers.

To make Research & Innovation outputs useful, usable and used, we promote new technologies emerging from European Commission funded Research and

Innovation (R&I) projects which provide secure and standardised solutions. We assess their market and technical readiness levels to improve their impact.

We map, test and promote the adoption of interoperability and security standards which are necessary in building trust in the cloud market.

We educate our stakeholders through online tools and guides, and informative workshops to promote the adoption of cloud computing.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

The adoption of both standards and benchmarks are vital for the continued growth of the cloud service market. This should be standards-based, avoids vendor lock-in, be fairly priced and open up the market to more players because:

- Standards allow a phased approach to cloud adoption using hybrid cloud technologies, and promote vigorous competition across this market.
- Standards facilitate more accurate price-performance benchmarking helping cloud buyers make purchasing decisions.

With more open source standardized solutions tailored for market requirements, R&I project outputs can really contribute to and drive the adoption of cloud computing for government, business and research. With more educated stakeholders, this can lead to a more resilient cloud market with fair, transparent pricing.

CREDENTIAL

Project acronym & name

CREDENTIAL - Secure Cloud Identity Wallet

- credential.eu

The CREDENTIAL project addresses the need for a secure and privacy-preserving cloud-based identity management and data-sharing platform. The project puts users in full control of the data and attributes they want to share, while keeping their data hidden from the cloud provider, thus giving high authenticity guarantees to its data receivers.

Who is the service/solution designed for?

On the one hand, the CREDENTIAL project targets cloud and identity providers who are interested in extending their portfolio with privacy enhanced and authentic data sharing services by leveraging the software developed in the project. On the other hand, CREDENTIAL targets service providers to learn how they can indirectly benefit from the CREDENTIAL Wallet service by registering as a receiving endpoint for authentic user data, thus providing more trustworthy eBusiness solutions.

Additionally, the privacy-preserving features of the CREDENTIAL platform also make it very attractive to public bodies who are interested in extending their portfolio of eGovernment or eHealth applications for citizens.

What problem is the solution/service trying to solve for your company or customers?

Existing identity and access management services essentially require a user to choose between the benefits of using cloud-based services and privacy: on the one hand, users can put their identity information into the cloud and let it be managed, e.g. by social media or search engine providers, who have full access to the user's identity information and can trace all of their interactions. On the other hand, users can keep their identity information local, requiring them to keep local state and transfer this state to each single device from which they want to authenticate themselves to a service, resulting in worse usability and flexibility.

Our approach combines the best of both worlds. If the users' data are stored in the CREDENTIAL Wallet, these protected as a preventive measure by strong cryptography from the most prevailing threats in cloud computing, even from the provider itself. At the same time, data is easily accessible anywhere, anytime, and all communication devices without complex synchronization

and configurations work. In essence, the project provides a versatile and easy-to-use solution to securely manage personal data in the Internet.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

CREDENTIAL combines the best of the two existing approaches for the management of identities in the digital world. It allows users to use a cloudified identity management and data sharing platform, while still protecting their privacy and guaranteeing end-to-end confidentiality. That is, the cloud provider does not learn any privacy-sensitive information contained in the authentication credentials. Furthermore, users can define, on a very fine-granular level, which parts of documents they want to share with service providers or other users.

Additionally, the CREDENTIAL system also supports selective sharing of authentic data protected by digital signatures, i.e., the data receiver will still be assured of the integrity of the partially revealed information. Enabling end-to-end authenticity for selectively shared data is another new feature not available today and another added value of the CREDENTIAL Wallet. Especially with the upcoming of eIdas solutions and the establishment of the Digital Single Market in Europe, the CREDENTIAL Wallet can act as an enabler for a more trustworthy and privacy-friendly way of doing business in the digital world.

ESCUDO-CLOUD

Project acronym & name

ESCUDO-CLOUD - Enforceable Security in the Cloud to Uphold Data Ownership

- www.escudo-cloud.eu

Effective and deployable solutions allowing data owners to maintain control over their data when relying on Cloud Providers for data management.

Who is the service/solution designed for?

The goal of the ESCUDO-CLOUD project is to empower data owners as first class citizens of the cloud. This will be achieved by providing enforceable security, that is, techniques that wrap the data to provide a layer of protection to the storing/processing Cloud Service Provider, setting the trust boundary at the client side, which implies correct and trusted behavior only by the client.

What problem is the solution/service trying to solve for your company or customers?

ESCUDO-CLOUD is targeted to both data owners and Cloud Service Providers. The availability of technologies empowering users to maintain control over data can increase the adoption of cloud services to more users or more applications. Also, it can free the Cloud Service Providers from the worries of protecting data, allowing them to securely handle the data outside their own control.

An additional target is represented by developers of solutions for cloud data management, who can extend their tools with the support of the protection techniques developed in the project.

What problem is the solution/service trying to solve for your company or customers?

The outcome of the project is expected to provide significant support to social innovation. Situations where sensitive information about the user is outside her control are going to be reduced. As evidenced in the project acronym, the goal is “to Uphold Data Ownership,” and this aspect is consistent with the evolution of ICT toward a scenario where users are empowered and able to control their own data.

The availability of technologies able to offer strong protection guarantees on outsourced data will then support a large variety of applications that are

becoming increasingly common thanks to the deployment of a continuously more varied landscape of IT devices.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

ESCUDO-CLOUD, empowering users with control over data, will remove possible concerns that today may limit cloud adoption, enabling users to rely on the cloud with confidence for a variety of applications and data.

ESCUDO-CLOUD will be beneficial to both data owners and Cloud Service Providers. Data owners will be enabled to outsource their data while maintaining control over them, with the ability to regulate access to them and share them with other users in a selective way and with assurance that their data will remain protected from the Cloud Service Providers. Data owners will then be able to rely on Cloud Service Providers and use their services for a wider range of applications. This will benefit both companies as well as individual users. Cloud Service Providers will significantly benefit, in addition to the increased market penetration that robust data ownership would provide, from reduced regulatory risks, audit costs, and general security threats that they would have to face in the absence of such protection.

MUSA

Project acronym & name

MUSA - MUlti-cloud Secure Applications

- www.musa-project.eu

The MUSA project provides an integrated tool framework for DevOps and Agile engineering of (multi-)cloud based applications, addressing security in all its phases: design, deployment and operation. The framework supports risk analysis and selection of secure cloud services, and is able to automatically deploy and monitor distributed components and create an application Service Level Agreement.

Who is the service/solution designed for?

The main targeted users are **DevOps teams** covering four main roles:

- **Application developers (including architects)** that need tools to easily design multi-cloud applications, not only according to functional features, but also taking security features such as data confidentiality, data integrity, data access and data location into account. They also require security mechanisms implemented in the applications, to enforce security at runtime.
- **System operators** that need to exploit cloud service combinations as much as possible and require tools to automatically select the best combinations, based on the functional and security needs of the application and to automatically deploy the appropriate components.
- **Service administrators** that need to monitor the correct operation of the application (fulfilment of SLA), including the security features, in order to react to security incidents as soon as possible and to keep the users properly informed.
- **Business managers** that have overall responsibility for the business aspects of offering cloud services to cloud service customers.

The four roles need tools that together can better integrate a seamless assurance of security in the applications.

What problem is the solution/service trying to solve for your company or customers?

The main goal of MUSA is to support the control of security in distributed applications over heterogeneous cloud resources, through a security framework that includes methods and tools for integrated security assurance

in both engineering and operation.

The main features on offer ease the processes of:

- Multi-disciplinary Risk analysis to better identify the required security controls in the application components.
- Selection of cloud services by taking into account the security controls that the services have to offer.
- Automation of the creation of the SLA requirements of the application. By composing the SLA requirements of the distributed components.
- Automation of the deployment of the distributed components in heterogeneous cloud services.
- Automation of the monitoring and enforcement of the security behaviour granted in the SLA through the use of agents within the application components.

All these processes will be seamlessly integrated in a unique Kanban-style Dashboard that is able to encompassing a number of tools that can also be used separately. The framework will reduce time-to-market and shorten the gap between the Development and Operations for a timely reaction to security incidents at runtime.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

The data security incidents in multi-cloud applications will be reduced through the assurance of a secure behaviour of individual cloud-based components and the overall application, even if the data is processed and/or stored by untrustworthy or opaque cloud providers.

The cloud consumers' trust in clouds will be enhanced by the provision of tools for expressing their security needs and keeping them informed on the security and performance faults of the multiple cloud services in use.

Application developers will be able to model the multi-cloud application, based on the functional and security features on offer in the SLA, as well as to embed application component mechanisms to enforce security at runtime.

System operators will be able to automatically discover and select the best cloud service combinations by balancing performance and security.

Service administrators can assure the secure behaviour of multi-cloud applications and minimize the security risks while keeping the users informed.

Business managers will be able to make better-informed decisions when selecting cloud services.

OPERANDO

O{P}ERANDO
online privacy enforcement, rights assurance & optimization

Project acronym & name

OPERANDO – Online Privacy Enforcement, Rights Assurance and Optimization

- www.operando.eu

The OPERANDO project is able to take significant and complex responsibilities from Governments and Service Providers by:

» Holding sensitive Personal Data offsite.

» Ensuring compliance with evolving data protection legislation.

» Holding data using a different Trust Model: an open source organization that exists for trust.

OPERANDO offers service users control over their data in that:

» Consent of service users is explicit.

» The ability to express personal preferences regarding data is available.

» A third-party in the unequal power relationship between local government and service user is introduced.

OPERANDO enables new business opportunities because:

» Data can be used for analysis and hence offer improved services.

» Anonymised Data can be shared with the user's consent to facilitate research.

Who is the service/solution designed for?

» Business to Consumer - B2C: consumers, users of social networks and B2C online services.

» Government to Consumer - G2C: Public administrations, Government, Health/social care and Regulated business entities.

What problem is the solution/service trying to solve for your company or customers?

B2C:

» Consumers are overpowered by the aggressive privacy invasion practices of Internet giants.

» The "You are the product" phenomenon – free services tempting customers to divulge vast amounts personal information that is monetized by OSPs.

» Consumers are not capable of keeping track of the changing permissions and privacy settings.

» Aggressive tracking of customers across sites and platforms, accompanied by intrusive behavior profiling and advertisements.

» Consumers do not partake in the benefits from monetization of their private data

G2C:

» Government institutions need to hold personal data. However, they have a duty to be transparent in their use and need to get consent from the data subjects.

» Lack of transparency with what is done with the provided data and "all or nothing" consent models.

» Managing personal and health data according to regulations is both complex and money consuming, especially when the regulation changes and these change affect the Health Information System.

» Existing regulations are both complex to understand and to implement, and changes to these laws require costly measures to remain compliant. This provides a strain as costs need to be contained.

» The data which is held on citizens could be used more effectively, for example in research or to improve services. However, this requires funding, improved data management and changes to policies.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

For end users OPERANDO provides the ability to manage all online privacy issues in an intuitive web-based dashboard. The user can set their User Privacy Policy (UPP) according to their preferences, which will be transparently enforced for each of the user's devices. The service will be free to users and simple to enrol.

For Service Providers: consuming privacy services will grant the ability to benefit from: i) Cost-effective compliance with privacy regulations; ii) Access to a lucrative user base and big data analytics reports; iii) Avoid assumed consent, and inadvertent exposure of unsolicited information; iv) Easy requests for information, allowing sharing between organisations for co-ordinated care; v) Sensitive Personal Data is held offsite; vi) Compliance with evolving data protection legislation is ensured.

For Data Regulators OPERANDO will provide access to the human- and machine-readable privacy guarantees of the Service Providers, and the ability to input privacy regulations in a similar form. This will allow an automated audit for compliance with the relative regulations. The OPERANDO project has engaged consumer rights and standardization organizations, endorsed by the EU, as members of its Advisory Board, and will act to position the OPERANDO platform for endorsement by European governments.

PRISMACLOUD

Project acronym & name

PRISMACLOUD – Privacy and Security Maintaining Services in the Cloud

- prismacloud.eu

PRISMACLOUD provides a box of five flexible tools, fully encapsulating strong cryptographic functionality, from which secure and privacy aware cloud services can be constructed. We address storage and data sharing security, data minimising and privacy providing authentication and authorisation mechanisms, topology certification, anonymisation, and an encryption proxy for legacy applications.

Who is the service/solution designed for?

We target individual and organisational end users, as e.g. administrations, health systems, and other community cloud users with common interest or particular compliance requirements, as well as businesses of different sizes and operating in different markets. We specifically address small and medium-sized enterprises, a sector with enormous economic growth potential enabled by the scalability of cloud services. We also want to address cloud providers that might be interested in providing your secure and privacy preserving services for the customers, compliant to the upcoming European General Data Protection Regulation, GDPR

What problem is the solution/service trying to solve for your company or customers?

In a post Snowden world, the currently prevailing threat modelling, with its focus on outsiders (hackers, rogue criminals etc.), is probably insufficient for modelling privacy threats in the cloud context. We assume that the "nature of clouds" requires the consideration of an expanded threat posture represented by insiders, e.g. the cloud processor, or other parties down the cloud provisioning chain. This concerns not only the actual (private) data of an end user, but any Personally Identifiable Information (PII), including metadata that accrue by accessing the cloud and performing operations on-line. Several groups of end users are currently barred from moving to the cloud because of the strong confidentiality required for their data and processing. In particular, the upcoming GDPR will require data controllers to keep precautions for the protection of PII which might only be practically realised by the use of strong cryptography.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

End users, such as individuals and organisational end users, including administrations, communities, and commercial enterprises, can potentially benefit from security and privacy in the cloud that is not only supported by contractual provisions – but proactively guaranteed by cryptographic measures. Such measures allow cloud customers to retract data from a cloud provider, or enforce the deletion of data at a cloud provider at their own discretion, without depending on good will and cooperation. Thus, several of our solutions support a re-empowerment of end users in the cloud context.

But also on the cloud provider side, our solutions can provide their benefit: Cloud providers will be able to provide advanced services to end users that value privacy and governance in the cloud. Cloud providers ("processors") will be able to provide "GDPR compliance as a service" to their customers, and will also reduce the responsibilities which would be imposed upon them in the case of processing PII in plaintext.

PaaSword

Project acronym & name

PaaSword - A Holistic Data Privacy and Security by Design Platform-as-a Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications

- www.paasword.eu

The PaaSword project introduces a novel data privacy and security by design framework with the objective to protect sensitive data stored in the cloud. PaaSword enables security annotations, transparently through an IDE, transformed into context-aware security policies that enforce access control, cryptographic protection and physical distribution to secure the privacy of sensitive data.

Who is the service/solution designed for?

PaaSword extends the Cloud Security Alliance's cloud security principles by capitalizing on recent innovations in virtual database middleware technologies, which introduce a scalable and secure cloud database abstraction layer with sophisticated data distribution and encryption methods. PaaSword provides encrypted and distributed storage, as well as context-aware access control, constituting a valuable asset for any Platform-as-a-Service provider. PaaS providers can easily adopt the innovative PaaSword solutions and thus deliver added value to their clients, with respect to the protection of next generation cloud applications against internal and external adversaries, in a quest to alleviate the cloud adoption concerns of the modern enterprise.

What problem is the solution/service trying to solve for your company or customers?

The adoption of PaaSword brings about new access control mechanisms that incorporate dynamically changing contextual information into access control policies and context-dependent access rights, which along with the encrypted and distributed storage support, consolidate the perfect fit for the dynamic cloud computing environment. Moreover, PaaSword brings all adopters one step closer to compliance with very demanding security regulations, such as the EC's General Data Protection Regulation (entering into force on the 25th of May 2018) which enforces strict penalties for enterprises that fail to protect their end-users sensitive data. In brief it offers: i) a searchable encryption scheme for secure queries support; ii) policy-based access control & context-aware security models; iii) governance capabilities for ensuring the validity of access control policies; iv) a dedicated IDE plug-in for injecting code-level

annotations that associates these policies with methods that provide access to sensitive data, v) a novel policy enforcement middleware that extends the well-known attribute-based access control paradigm with semantically-rich context information, vi) unique distributed storage across IaaS providers for disentangling data objects that might reveal sensitive information to internal or external adversaries, vii) the PaaSword holistic framework that integrates all of these novel offerings.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

Current cloud applications and storage volumes often leave information at risk to theft, unauthorized exposure or malicious manipulation. The most critical part of a modern cloud application and services is the data persistency layer and the database itself. To remedy this risk, PaaSword introduces a holistic data privacy and security by design framework, based on distributed and encrypted data persistence and sophisticated context-aware access control mechanisms in cloud-based services and applications. Unlike any other solution, PaaSword supports both developers of cloud applications with code annotation techniques and DevOps with the necessary modelling and management tools for achieving an appropriate level of protection for their cloud application's data, even in cases where sensitive information resides on untrusted IaaS providers. Thus, PaaSword enables enterprises to unlock the valuable business, economic and operational benefits of migrating to the cloud, as it generates the confidence of individuals and corporate customers in cloud-enabled services and applications. These valuable business benefits cannot be unlocked without addressing the new data security challenges posed by cloud computing.

The long-term expectation of the impact of the project is to assist in the accelerated adoption of cloud computing technologies, and to see a paradigm shift of European industry towards security and privacy.

SWITCH

Project acronym & name

SWITCH - Software Workbench for Interactive, Time Critical and Highly self-adaptive Cloud applications

- www.switchproject.eu

SWITCH addresses the urgent industrial need to develop and execute time critical applications in Clouds. Applications such as disaster early warnings, collaborative communication and live event broadcasting can only realise their expected business value when they meet critical requirements in terms of performance and user experience.

Who is the service/solution designed for?

SWITCH targets:

- Software industry: to support software development and consultancy companies in delivering time-critical applications and services.
- Cloud service providers: to enable SLAs for time-critical services.
- Telecom service providers: for network providers and infrastructure operators.
- SMEs and entrepreneurs: for operating and developing their own applications with time critical requirements.
- Education organisations / Universities: for education/training purposes.
- for a wide collection of domains that require time critical services: Time critical applications in specific domains.
- Technology vendorsincluding API management companies SDN and virtualization vendors, Telecom-managed service providers, and wireless/ mobile infrastructure providers.

What problem is the solution/service trying to solve for your company or customers?

The very high requirements posed on network and computing services, particularly for well-tuned software architecture with sophisticated data communication optimisation, impies that development of such time critical applications is often customised to dedicated infrastructure, and that system performance is difficult to maintain when the infrastructure changes. This fatal shortcoming in the existing architecture and software tools yields very

high development costs, and makes it difficult to fully utilize the virtualised, programmable services provided by networked Clouds to improve system productivity.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

SWITCH aims to improve existing development and execution models of time critical applications by introducing a novel conceptual model (application-infrastructure co-programming and control model), in which application QoS/QoE, together with the programmability and controllability of the Cloud environments, can all be included in the complete lifecycle of applications. Based on this conceptual model, SWITCH provides an interactive environment todevelop applications and control their execution, a real-time infrastructure planner todeploy applications in Clouds, and an autonomous system adaptation platform to monitor and adapt system behaviour.

SERECA

Project acronym & name

SERECA - Secure Enclaves for REactive Cloud Applications

- www.serecaproject.eu

The SERECA project aims to substantially improve the state-of-the-art in cloud security for interactive, latency-sensitive applications by seamlessly integrating the new security features provided by Intel CPUs - namely: Intel Software Guard Extensions (SGX) - in a standard cloud stack.

Who is the service/solution designed for?

Virtually all service providers who cannot trust their cloud provider not to tamper with their applications. Traditionally, to trust a service (implemented via an application) the complete system stack has to be trusted, i.e., the hypervisor, the operating system of the host system, the operating system of the VM and all users with root access to these components. The SERECA platform only implies the trust of the application itself and its libraries: the SERECA platform provides application-oriented security. SERECA itself is part of the libraries linked to the application.

What problem is the solution/service trying to solve for your company or customers?

Using the new security features provided by recent CPUs requires massive effort on the developer's side. SERECA makes CPU extensions readily available via the APIs of a flexible software framework, namely Vertx. By doing so, SERECA ultimately enables application developers who are not security experts to take full advantage of hardware-based security features at no extra cost.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

End users will be protected from insider (e.g. the cloud provider or the system administrator) attacks.

SecureCloud

Project acronym & name

SecureCloud - Secure Big Data Processing in Untrusted Clouds

- www.securecloudproject.eu

SecureCloud addresses the confidentiality, integrity and availability of applications executed in the cloud. Data at rest or in transit on the network is already nowadays protected by encryption. The main problem that we face is how to ensure the confidentiality of data while being processed. Our approach is based on upcoming hardware extensions of commodity CPUs.

Who is the service/solution designed for?

Our end users are those who need to process massive amounts of data in a timely and secure fashion. The project focuses on the power grid domain.

What problem is the solution/service trying to solve for your company or customers?

Hardware extensions of commodity CPUs are not easy to use. A large fraction of application developers lacks the skills that are needed to fully exploit them. SecureCloud makes CPU extensions readily available via a pre-packaged container. By doing so, SecureCloud enables developers to deploy their applications in a secure way at no extra cost.

How can the solution/service help you become more efficient, more secure, faster or cost-effective?

End users will be protected even from attacks launched by privileged users.

Published by

www.cloudwatchhub.eu

Services for

Small & Medium Businesses
Large Enterprises
Public Sector & Government
Cloud Service Providers
Data Regulators

Keywords

Data Security
Data Cryptography
Data Privacy
Critical Applications
Multi-Cloud Environments

www.cloudwatchhub.eu/cloudsecurity
bit.ly/DPSPcluster

European Commission

These projects have received funding from the European Union's Horizon 2020 research and innovation programme.