

The architecture for data, security and application in Digital Earth platform

Fang Miao^{1,2}, Wenhui Yang¹, Ansheng Ye², Huayue Chen¹

¹ Institute of Spatial Information Technology, Chengdu University of Technology

² Research Institute of Big Data, Chengdu University

E-mail: miaofang@126.com

- **Abstract.** Digital Earth platform is an application, service and decision support system, which integrates geo-spatial data acquisition, transmission, storage, processing, analysis, statistics and visualization. It realizes comprehensive management and widely application of different kinds of huge earth data under the geo-spatial framework and in a open environment . It should consider the continues growing of data and applications, as well as data security. According to the issues of how to safely use spatial data in Digital Earth platform, an architecture for data ,security and application in Digital Earth platform was proposed in this paper. We call this architecture DOA(DOSA). In the digital earth platform on its goal is the Trusted Data. DOA(DOSA) and Trusted Data can provide data management, security grantee, application supporting for Digital Earth platform.
- **Key.** Data Oriented Architecture(DOA), Digital Earth platform, Trusted Data Data-Oriented Security Architecture(DOSA)

1. Introduce

1.1 Background

In 1998, U.S. Vice-President Al Gore articulated a vision of “Digital Earth” as a multi-resolution, three-dimensional representation of the planet that would make it possible to find, visualize, and make sense of vast amounts of dereferences information on the physical and social environment. Such a system would allow users to navigate through space and time, access to historical data as well as future predictions based for example on environmental models, and support access and use by scientists, policy-makers, and children alike [1]. Since then digital earth was largely developed globally. Huadong Guo [2] gave Digital Earth a definition in 2008. He claimed that Digital Earth is a mega-data system about the Earth in regard to the information of natural and human society, the model of earth evolvement and society development, information technology system, and the geo-spatial information obtaining system; is a development of geo- and social science in the computer technology,



Web system technology, Web sensor technology, satellite remote sensing technology, global positioning system, geography information system, virtual reality technology, data storage and database technology.

Google Earth which was produced by Google Co. in June 2005 brings digital earth technology application into a new stage. Google Earth technology made a great progress by integrates international computer technology and 3S technology in the aspects of data and application. Google fully utilizes his powerful search engine and Web server system around the world to successfully realize the mega-remote-sensing-data based functions, such as browse, query, measure, path analysis, location-based service (connected with GPS) and so on, and realize serving the public with the information by popularizing the application of digital earth science and technology for the common user on the Web.

Digital Earth platform is an application, service and decision support system, which integrates geo-spatial data acquisition, transmission, storage, processing, analysis, statistics and visualization. It realizes comprehensive management and widely application of different kinds of huge earth data under the geo-spatial framework. Digital Earth platform includes all kinds of data and information with and without geography coordinates, Including the following data (1) space-based dimensions of different regions; (2) region-based dimensions of special requirements; (3) time-based dimensions of different spans; (4) science-based dimensions of different purpose; Digital Earth platform need to adapt in and grantee and rapidly growth of data and application. It should consider the continues growing of data and applications, as well as data security.

1.2 Main Factors Considered

The era of Big Data platform for the Digital Earth is the use of mass, multi-resolution, long phase, multi-type Earth observation data and social economic data and its analysis algorithm and model building of virtual earth, its data acquisition and organization, analysis, application embodies the characteristic of the large data. A new generation of Digital Earth platform is not generally interpreted as "put the earth into a computer," and in today's era of Big Data, we can think of Digital Earth is earth's big data. We can pass on the Digital Earth platform for massive spatial data efficiently and social economic data organization, to streamline the data space for scientific information mining and analysis. We may face the following issues:

(1) Digital Earth and Smart Cities in Big Data Era

Previously we only deal with very small parts of data in some applications. The era of Big Data of Digital Earth and Smart City, is not a simple earth or city data into the computer but to pass on the Digital Earth platform for massive spatial data efficiently and social economic statistics organization, to streamline the data space for scientific information mining and analysis. Data island or data chimney become more and more serious. Sharing data across industry, cross-scrotal, cross-regional exchange is difficult. In the agricultural civilization era, the core resource is land; In the era of industrial civilization, the core is energy resources; In the Internet Big Data age, the core is data resources. Break "data island", "data chimney", to revitalize the flowing data is imminent. At the same time some fundamental problems raise, such as data transaction, data rights, data ownership, data profits belongings, etc.

(2) Big Data management

Emerging services such as Cloud Computing, Internet of Things prompted data type and size of the Digital Earth platform is growing at an unprecedented rate. We are facing data with features of huge, different structure, static & dynamic, different sources, real-time & historical, public & private, etc. Formal Big Data era, data from simple processing object into a fundamental resource. How to better manage and use the Digital Earth platform of big data has become a common topic. Big Data scale effect for data storage, management and data analysis application has brought great challenges.

(3) Data fusing and processing

The era of Big Data exist multi-source heterogeneous data; widely distributed; dynamic growth; first the characterizes of the data after the model. The extensive existence of data makes data are increasingly spreading, and there are multi-dimension, multi-phase and multi-style earth observation data and ground observation data in the Digital Earth platform. In order to carry out data integration, data analysis need to be on the Digital Earth platform widely heterogeneity is mainly reflected in the data. 1) Data types from mainly structured into structured, semi-structured, and unstructured; 2) Different types of data integration (social and economic data; 3) The diversity of the way of data changes in the data source. With the rapid development of mobile terminals, mobile phones, tablet PC, GPS and other explosive growth, the amount of data and the data produced with obvious characteristics of time and space. Data growth Apps, Apps accumulate data.

(4) Data security problem

Putting forward along with the "Internet Plus" plan of action, the mobile Internet, Cloud Computing, Big Data, such as the Internet of Things will be as an important thrust of economic development in the new period, the information system facing the environment more open, more demanding for data and information security. In open environment, safely storage of data and safely delivery, traditional methods are facing great challenges. Unauthorized or using system leaks to access data become more dangerous. Digital Earth platform requires a new generation of data security solutions in open internet environment. At present, most of the Digital Earth platform in the data center involved in data security, refers to the use of the data backup, data disaster recovery techniques to guarantee the data is not lost, don't be destroyed, but still unable to prevent dangerous behavior, such as unauthorized access to data and information leaks risk. So closed environment security method in open environment is facing great challenge, how to guarantee the Digital Earth platform of data security in open environment become an important research topic.

1.3 The New Architecture of Digital Earth Platform

Digital Earth platform needs to have a new mechanism. In the open environment, the core of information security is the security of the data, to carry out data and data as the core of the data security system research is very necessary. Facing the open Internet environment, the Digital Earth platform needs to have a lower level, directly to the architecture of data to ensure data security and the application. In this paper we consider that the Digital Earth platform based on open environment data security problem, design the application data security mechanism, introduces the technical architecture for data(DOA) [3]. And build low-level architecture, try to solve the data ownership, information sharing, data management, system function expansion, the big support data analysis and mining, software engineering,

information security, and to guarantee the data owner interests, so as to build the era of Big Data Digital Earth platform security mechanism of data access.

2 Data Safely To Be Used: The Goal of Data-Oriented

Big data era in order to solve the problem of space information network service application in the G/S (General browser / Services cloud) model supported by the Cloud Computing, also known as Port/Cloud model. DOA and Port/Cloud model diagram is shown in figure 1. From the perspective of data, cloud computing is the data storage services, more is IaaS and DaaS, through distributed and virtualization technologies, the infrastructure and data (I+D, Infrastructure plus Data). For end users to provide flexibility, quantifiable, personalized data and computing services. Everything in the cloud, including all of the infrastructure, such as network, servers, storage devices, etc., more important is including all the data, the network world and physical world of data and so on.

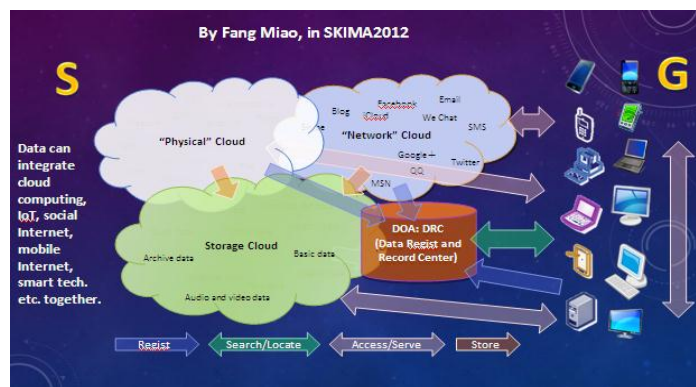


Figure 1 Data view: integrate all techniques

The architecture of the Digital Earth platform, we use the data and data as the core oriented thinking, data security problem in view of the open environment, leading into the data-oriented technical architecture, data access mechanism of building security. Figure 2 shows the data in the core position in the platform architecture.



Figure2 Data As A Kernel

In under the guidance of the data and data as the core, data processing and related technologies, as shown in figure 3:

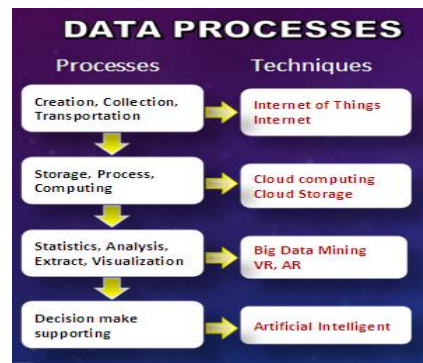


Figure3 Data Processes

Digital Earth platform with the data system is an ecosystem. It means that data and applications can be changeable, growth and sustainable development, and self-adaptive. According to the data oriented and data as core ideas to establish ecological system, various applications, including ecological data ecosystem is like as "fertile and rich data soil to grow with plentiful and luxuriant application forest". Ecosystem need to construct a logical data resource pool, support the big data platform and fragmentation and increasing the application of the support data sharing and the system can be extended. Based on the data: all measurable, all can be united, all operational, everything can be realized. Data security ecosystem as shown in figure 4.

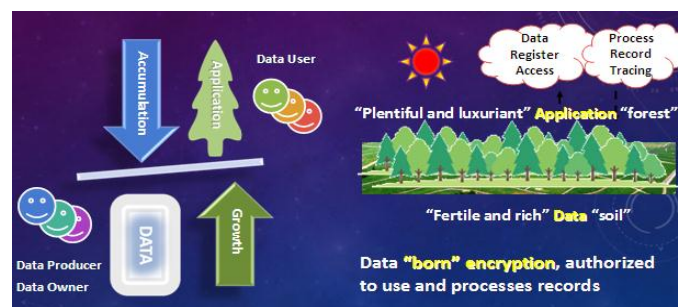


Figure4 Data Security Application Ecosystem

3 The Trusted Data and Platform——DOSA

Data-oriented security architecture based on the underlying architecture Digital Earth platform on data security system carries on the comprehensive design, including data management and application, etc. DOSA is built based on DOA, face data and based on data about the data security architecture, built up from the data protection to the mechanism of a complete set of license application. DOSA are based upon "cloud computing" and CA (Certification Authorization) / PKI (Public Key Infrastructure), as data encryption, "natural authorized the use of" for the principle, properties for registration and management of data, so as to realize the data security management and application. The purpose is to form a trusted data and its application in an open environment. DOSA is composed by DRC (Data Register and Recording Center), DAC (Data Authorization Center), DEC (Data Exception Control Center) and DAUs (Data Application Units).

3.1 Trusted Data

Emphasizes the trusted data from security protection object data itself establish credible mechanism, is the security solution of the future. Trusted data is different from trusted computing, trusted cloud computing and trusted computing environment. They all have in

common is through the security infrastructure to achieve the purpose of a can trust, strengthen the sense of security. The difference is that the former is on the object, credible, the latter from the environment and the means to achieve reliable. Trusted data is to stand in the angle of the data, with the support of cloud computing, based on the CA and PKI technology system, i.e. the data-oriented security architecture. Trusted data emphasize the object of information security, that is, to protect data itself. Trusted data, or DOSA, is an open environment of "data security applications" solution, is to build a "data security applications" ecosystem, is the basis of the data in the future architecture. Data can be trusted in an open environment. Data is protected and can be used. It is one of the solutions for future information security, is also the solution for Digital Earth platform.

3.2 Data attributes

Data shall meet the following basic characteristics: the concept of generalized data, and the life and attribute such as identity, security attribute, time and spatial attribute.

- (1) Generalized data: Who can be computer registration and registration of any things are called data.
- (2) Identity properties: Data ownership, that is, the owner of the data (data producers and data owners), friends (data user or licensee), strangers (unauthorized and stay to the authorized person) and the enemy (not the authorized person, blacklist).
- (3) Security attribute: Data has the protection function, to "wear armor", presenting an encryption, have different level of encryption and depth, the use of the data to be authorized.
- (4) Time and space attribute: The generation of data, authorization and the use of time and space.

Data is the basis of the application and not dependent on the specific hardware and software environment, the same data to support different applications. For convenience of management, we to store and transfer into keeping the encrypted data and authorization in should be used when using decrypt application state. Data only when the application state is in a state of decryption, once completed or left the application environment, or by the application of the new data, data shall be immediately into the encrypted data, fully guarantee the security of the data and the use of authorization.

3.3 Data-Orient Security Mechanism

Core mechanism of data security and data security applications include data registration, data encryption, natural authorized the use of data, data record, data tracking back, etc, the relationship between them is shown in figure 5.

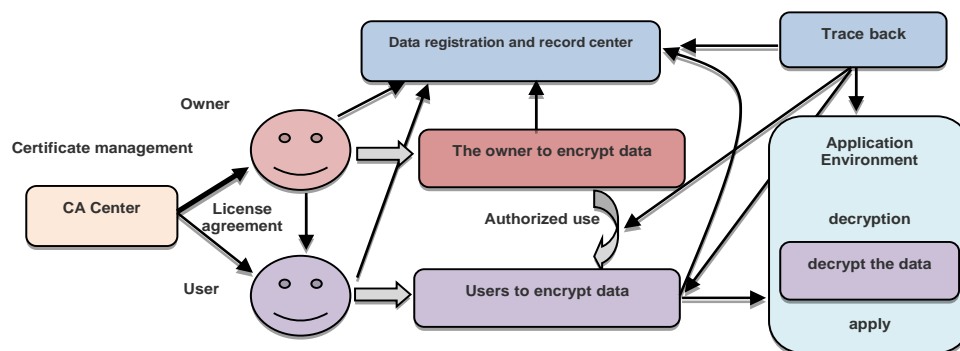


Figure 5 The relations of data ownership, security, applications

All kinds of fragmentation data platform and application can be compared to "fertile and rich data soil to grow with plentiful and luxuriant application forest". Accumulated and rich in a variety of data is defined as the soil of data. While all kinds of fragmentation, personalization and applications are defined as growing forests. The application forest can be ecology, flourishing and sustainable development. To establish an ecosystem of data platform with fragmentation applications and protection of data, is a solution of effectively deal with the growth, adaptive, the mechanism of management and sustainable development between data and applications. The Digital Earth platform with security and ecological application and service system on an open environment is built as an ecosystem, which is based on coordinating of the relationship among data, people and applications. Data security applications of ecological system consists of the following main components: CA (user authentication center), DRC (data registration center), PKI, DAC (data authority center), DEC (data exception control center), DWR (digital watermarking records center) as well as DAUS (data application units) etc., shown in figure 6.

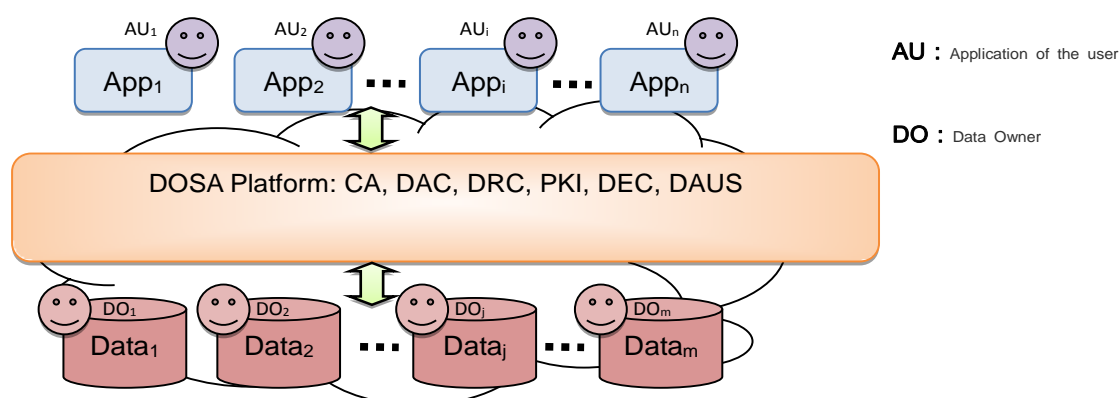


Figure 6 Data security applications of ecological system

3.3.1 People Identity Certification

Every people who do activities in cyberspace have an identity. This identity is certification authorized (CA). CA provides each person a digital certificate, that is a public key and a private key. One of the core idea of DOSA is to determine the data to the user, the relationship between the ownership of the data need to be clarified. This will require new users to participate in the activities of the network to the registration and identification. DRC to all registered users, while user identity authentication by CA. CA authentication using third-party CA authentication center, digital certificate to network users by the public and private keys. The private key in the form of a variety of safe distribution to each user, while the public key is stored in the data in the registration center.

3.2.2 Data Ownership

Data ownership is the relationship with people. Each data has its own rights ownership. The data can be divided into three kinds of relationship: data owner, data producer and data user. Other data can be set to agents in liability. Data ownership as shown in figure 7.



Figure 7 Data Ownership

Data owner, who owns all rights of the data. In general, who pays for the data, who is the owner of the data and purchase data only authorized users and owners.

Data producer, who is under a kind of contract with data owner to produce the data.

Data user, who is authorized by data owner to use the data.

The three relationships: they can be the same person, also can be different people and can also according to the situation changes to the data responsibility among each other.

Data agent, who is authorized by data owner to execute some functions for data owner, such as data manager, data seller, etc.

3.2.3 Data Born Encryption

All the participants on the digital earth platform has a unique network id (digital certificate), such data can be in accordance with the data owners intend to implement encryption. Once the data produced, DOSA platforms need to clear two things: First is to determine the owner of the data and the producers of data; The second is to encrypt data, to prevent others to steal. Under normal circumstances, the data of the producer is the owner of the data. No matter in storage or transport state, data is to keep the encryption. In other words, with the public key encryption, determine the owner of the data, and the data encryption present; use the private key encryption, identified the data producer, data producers in general is the data owner. Data born encryption is that data is encrypted just after data is produced. Data keep in encryption no matter it is in storage state or in transmitting state. The encryption is in concerned with data ownership. The encryption key is the public key of a data owner, or the public key of an authorized data user. Using symmetrical encryption for large data, while the symmetrical key is encrypted by the public key.

Data natural encryption use Certificate Authority and Public Key Infrastructure, With the data owner's public key to encrypt data, encrypted data can be placed in any public space, such as stored in the public cloud, Only the data owner himself by his own private key can decryption data. With the public key encryption, the owner of the data is determined, and the data encryption present; with the private key encryption, the data producer is determined, as shown in figure 8.

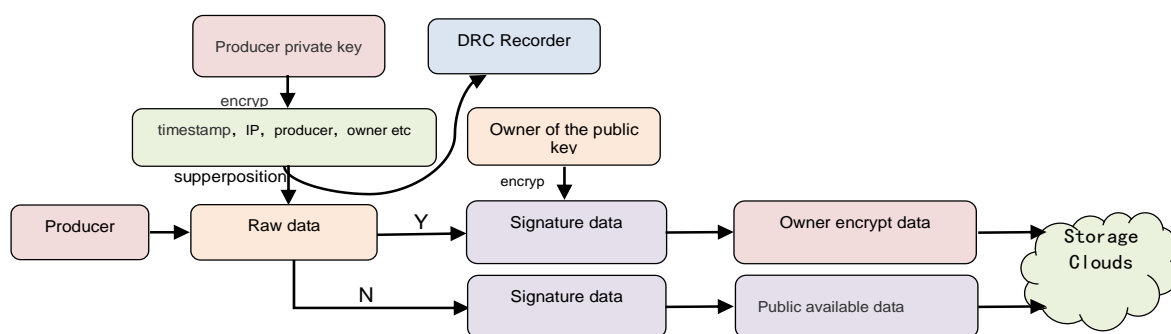


Figure8 The data flow chart of encryption by nature

3.2.4 Data Born Registered

Data is also born registered. Data resist is get unique ID and URL location. The registered data can be seen and can be searching, can be indexed, and can be analyzed. Encrypted data becomes available to use if registered. The performance of using registered data needs cloud computing. The security of registered data needs platform authorization.

DRC is the core component of DOSA, use all sorts of data attribute information of registration, including the security of the data attribute information and right of data information, etc, and the use of data process record. DRC also reserves the rights of all the data and the application of the user's public key. DRC used to construct the logic data resources pool, through the establishment of the index and search engine, implementation, implement the data and application of management and service. A DRC can be associated with other DRC, so as to realize data sharing. Through CA digital certificate and private key safe distribution to individuals with a variety of forms, the public key is stored in the data registration and record in the center. As shown in figure 9.

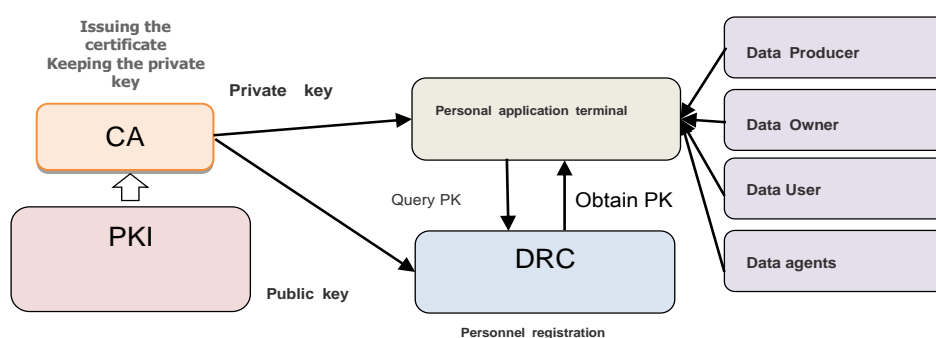


Figure9 The identity authentication In DRC

3.2.5 Authorized the use of data

DAC is the key to DOSA parts, used for authorization management data. Data in the generation, storage and transmission is encrypted and not to be used, and authorized users in the use of the data is decrypted and accessible. User needs the data owner authorization to use data. The authorization for a legal data user, needs both law contract permission and technology ownership transfer .Authorization of the data, is data ownership change, is the process of data decryption and encryption, with the data owner of the reoccupy after private

key to decrypt the data using the public key encryption. Authorization process to go through the watermark and registry data for recording and management. For larger volume data, take the symmetric key encryption method, authorization process is carried out on the symmetric key. The copy of data is necessary, the time and space consumption will need cloud computing and fast hardware support, but now it is possible because the price is very low. Authorization of data is the data of the ownership change, that is the process of data decryption and encryption, In which private key to decrypt the data owners reoccupy after data users (the licensee) the public key encryption, The data registration and authorization process records center for recording and management, In some permission, may also be authorized by superposition of watermark information. We based on the dynamic behavior of the data record and tracking, can find the data to a third party without authorization.

3.2.6 Data Security Applications

Make sure data security application environment general considerations decrypt the data in memory, to the memory data by means of a variety of security and not into stealing. Data is only decryption in an application. Open environment, to do the security of the data itself, and can safely use, the first is to encrypt data, the data should have the characteristics of "natural encryption, authorized the use of. Might as well assume that data in use is not encrypted state, then the data is not in use should be encrypted. Set data, therefore, has two states: when the storage and transmission is in a state of encryption "data" and authorized the use of the "application" in a state of decryption. DOSA as a mechanism, we must ensure that data can be in a state of the two and authorization, and encryption technology. DEC is an important part of a DOSA, adaptive management for use in data resources, ensure the uniqueness of the data and consistency, supervision and disposal of all kinds of abnormal behavior data. DOSA based on data encryption innate, authorized the use of the concept of, Data access on the basis of the data security attributes and the identity of visitors, by applying the authorization, user authorization, and then determine the authorization of the data, according to the authorization of way and the application environment, provide the decryption key or decryption algorithm, realize the safety of data is used.

3.2.7 Data Use Processes Recording

DWR will be in the form of the watermark data are recorded and authorized the use of process, together with the original data is encrypted management, facilitate tracing the source of data, accounts and data the unauthorized use of evidence. Data authorization processes and application processes should be recorded. The time stamp and space location should be recorded. Similar to Block Chain, DRC will record whole data events in its life circle. This will also take some consumption of time and space, but now we can endure it by cloud computing, etc. Once we find illegal data, we can trace and find the person who does not observe the contract. Using Big Data analysis of registered and recorded information, as well as the system log files, we can locate and find the real illegal person.

Can be based on the analysis of the recorded information and mining, to understand the use of the data, in some application scenarios can provide valuable information. Especially the authorized the use of process data, can trace data records, can help to understand the data of normal and abnormal use.

3.2.8 Data Value Assess

Big data era, a new generation of digital earth platform under the Internet + data plays an

important supporting role. Digital earth platform infrastructure, is actually the precipitation data in the platform all digital business, can we put every business use data to precipitate down. Analysis registered and recorded data information and using assessing model to calculate the data values.

Under this background, the data as an important resource, but if we don't flow will not be able to create value for sure, In data oriented architecture built digital earth platform allows data open, Shared, and financing can not only make social efficiency more effectively, and increase new blue ocean, new resources, let everybody can enjoy in the process of using the benefits of open data application data.

Data can be easily copied and transmitted, It belongs to you can copy and repeated trading assets, will become the world's most important asset; In essence, the value of the data by the extent of the circulation and has been applied. From another perspective, the data only in circulation and the collision will produce a higher value. Data is property and the owner should get paid by its value.

3.2.9 Discovery Data Violation

Data using the authorization is one of the biggest challenges facing illegal or illegal outflow data from authorized users of the data. There maybe some illegal or violation of using data. Due to the data users there, normally can't supervise data, Therefore, on the one hand, need through the establishment of rule of law and moral self-discipline to restrain illegal and irregularities, On the other hand, can only use data registration and record information to analyze and judge from whom data. According to data registered and recorded information, we can use Web spider or crawler to find data violation. To find illegal flow of data, must first determine the illegal data found the place and time, coupled with recorded data event in this paper, and the parameters of time and space, where can preliminary judgment data out. Further, you can through the large data analysis, to accurately analyze the offenders. This will become normal to patrol the network under the legal data application.

3.2.10 Data Records Tracing

Once we find illegal data, we can trace and find the person who does not observe the contract. We can according to the record contents of data dynamic behavior research data, analysis data, the dynamic behavior of the characteristics. Using Big Data analysis of registered and recorded information, as well as the system log files, we can locate and find the real illegal person. . Using big data analysis research and analysis of the data found abnormal behavior and call the police, the unauthorized data such as illegal use of data in time, judgment and tracking method, using the web crawler found illegal data and traces the offenders.

4 Applications and Prospects

DOSA, as a kind of data security concept and mechanism, is to ensure that the data in the data and application in the two aspects can be safe, reliable, convenient for management and use, can be applied in the traditional closed environment, enhance the data safety protection, and can protect the data in open environment safety and is not from unauthorized access. At present, the emergency command system in Si Chuan province people's government, geological disaster monitoring and management system and education resources public service platform and application system of Si Chuan province are applied the DOSA

architecture, expected to be effective application in the digital earth platform.

The related theory and method system of information security, data security, AAA technology about network security, the CA technology, PKI technology and key system, encryption technology, the reliable technology, as well as the continuous development of network space security, system security, application environment security technology, etc., can be used in DOSA framework, But need to be further from the Angle of the oriented data and data as the core, to comb, from data security concept, theory, method and the application of the protected data mechanism, etc., adaptability and in-depth study, in order to further improve the information security guarantee. DOA & G/S model support data growth applications as shown in figure 10

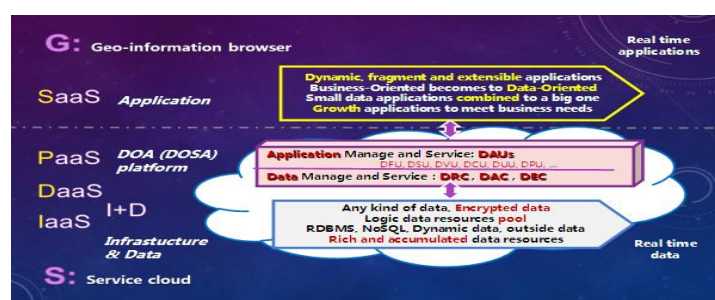


Figure10 DOA & G/S Model Support Data Growth Applications

5 Conclusion

Digital Earth platform needs an ecosystem for data growth and application growth. Open environment information security problems embodied in the data on the safety of digital earth platform of all kinds of big data security in open environment will be severely challenged. DOSA and Trusted Data can provide data management, security grantee, application supporting for Digital Earth platform. DOSA use the data-orient and the data as the core of the idea, set up data with the relations between the ownership of the user, use data "natural encryption, authorized the use of" method, By the CA, DRC, DAC, DEC, PKI, DWR, DAUS etc for data security management and security applications, Established from the data protection to the authorization mechanism of a complete set of application. Based on data-oriented security architecture of the digital earth platform may effectively solve the geospatial data security and respond to open environment, ownership, trading, sharing, management, privacy and other problems and challenges. Coordinating the relationship among data, people and applications, building a Digital Earth platform with security and ecological application and service system on an open environment, is the new architecture in the Era of Big Data.

References

- [1] Max Craglia, Michael F.Goodchild, Alessandro Annoni, Gilberto Camara, Michael Gould, Werner Kuhn, David Mark, Ian Masser, David Maguire, Steve Liang, Ed Parsons.Next-Generation Digital Earth*,A position paper from the Vespucci Initiative for

- the Advancement of Geographic Information Science. International Journal of Spatial Data Infrastructures Research, 2008, Vol. 3, 146-167.
- [2] Guo Huadong. DIGITAL EARTH SCIENCE PLATFORM: DESP/CAS .The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Beijing, 2008, Vol. XXXVII. Part B2,1089-1091.
- [3] AGRAWAL D, BERNSTEIN P, BERTINO E, et al. Challenges and Opportunities with Big Data-A Community White Paper Developed by Leading Researchers Across the United States [EB/OL].[2012-10-02]. <http://www.cra.org/crc/files/docs/init/bigdatawhitepaper.pdf>
- [4] Fang Miao. Data-oriented Architecture <http://baike.baidu.com/subview/649092/12822804.htm#viewPageContent>, 2014
- [5] Xueqi Cheng, Xiaolong Ji, Yuanzhuo Wang, etc. Big data system and analysis technology were reviewed [J]. Journal of software, 2014, 25(9): 1889-1908
- [6] Xiaofeng Meng etc. Big data management: concepts, technology, and challenges [J]. Research and development of the computer, 2013, (1): 146-169
- [7] Fang Miao, A preliminary study on the security architecture for data [J]. ZTE Communications, 2016, Vol.22 No.1:19-22
- [8] KRESIMIR S, HRVOJE O, MARIN G. The Information Systems' Security Level Assessment Model Based on An Ontology and Evidential Reasoning Approach [J]. Computers & Security, 2015, 55(6): 100-112. doi: 10.1016/j.cose.2015.08.004
- [9] GEORGE S, VLADLENA B, JEAN N E, et al. Individual Information Security, User Behaviour and Cyber Victimization: An Empirical Study of Social Networking Users [J]. Technological Forecasting and Social Change, 2015, (5): 320-330. doi:10.1016/j.techfore.2015.08.012
- [10] GURPREET D, ROMILLA S, CRISTIANE P. Interpreting Information Security Culture: An Organizational Transformation Case Study [J]. Computers & Security, 2015, (4):63-69. doi: 10.1016/j.cose.2015.10.001
- [11] AGRAWAL D, BERNSTEIN P, BERTINO E, et al. Challenges and Opportunities with Big Data-A Community White Paper Developed by Leading Researchers Across the United States [EB/OL].[2012-10-02]. <http://www.cra.org/crc/files/docs/init/bigdatawhitepaper.pdf>
- [12] XIAO X R, SUN X M, WANG X B, et al. DOSM: A Data-Oriented Security Model Based on Information Hiding in WSNs [J]. Information Technology Journal, 2009, 8(5):678-687
- [13] Yimin Liu. Private data access control mechanism based on access to the purpose of research [D]. Shanghai: fudan university, 2012