BLOCKCHAIN BASED DATA SECURITY AS A SERVICE IN CLOUD PLATFORM SECURITY

Magesh Kasthuri

Wipro Limited, Bengaluru, India

ABSTRACT

Blockchain is widely used for money related transaction and still there are many proven usecases across different industries like Retail in stock checks and order management, Manufacturing in good movement processing, Health care in patient database management to name a few. With this in mind, it is always important to understand the merits and demerits of both Public and Private Blockchain to understand their capabilities and limitations to decide which one is more suitable for an industry specific usecase implementation. In a Cloud based platform, data security plays a crucial role to cater to data protection and regulatory requirements and Blockchain can play an important role in this for accelerated workflow by providing 'data security' as a service capability.

KEYWORDS

Data Security, Blockchain, Cloud platforms, Data protection, Regulatory requirements

1. INTRODUCTION

In PermissionLess Ledger, user can login anonymously without revealing the identity and controlling the transaction rate can be done through a defined owner group. On the other hand, Permissioned Ledger has defined roles like Owner, Approver, Viewer/Reader and Administrator. These roles has defined workflow activities and controlled transaction processing is ensured in a Permissioned Ledger based Blockchain platform using these user roles. There would be more than one users present for each role so that speed of transaction is faster as compared to PermissionLess Ledger.

In a Multi-tenant cloud architecture, even the application environment is shared in a single workspace (subscription) there are restrictions to access the application and data (including the Virtual machines) and hence irrespective or public or private cloud environment, application and data security is ensured and contained within a limited group of known resources. Hence it is utmost important to have a robust data security service in cloud platform to accelerate workflow based resource access through some gatekeeper activities.

2. MULTI-TENANT APPLICATION DESIGN

A multi-tenant design is a horizontal demarcation between application groups to restrict accessibility of application and data between user groups and security groups. In terms of multi-tenant database design solution, there are many options like design multiple database for each application or design a single shared database with multiple schemas so that schema level user permission can restrict data access between them or even have a single shared database with shared schema where table level permissions can isolate each tenants of application group.

DOI: 10.5121/ijccsa.2021.11601

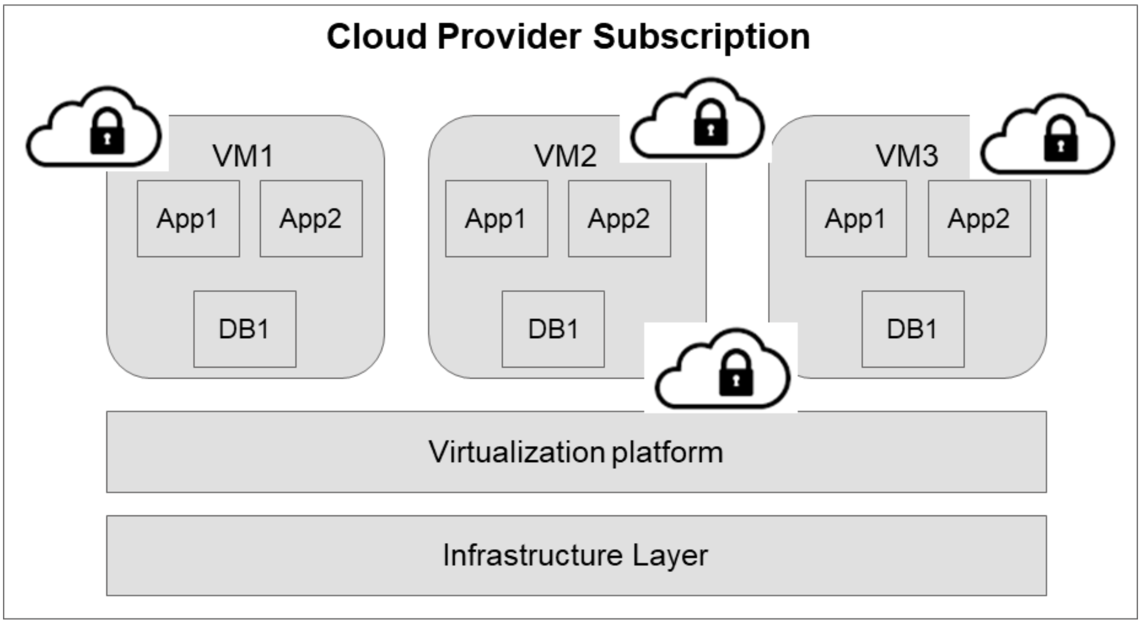

Figure 1: Multi-tenant application design with security

One of the key benefit of Multi-tenant design is cost effective as it still uses shared environment without compromising security and accessibility. It also simplifies overall integration design, re-usability of provisioning services through template; streamline the usability and central monitoring solutioning for support team without compromising privacy or data or application level security.

2.1. Key Drivers for Multi-Tenant Security Design

One of the key benefit of Multi-tenant design is cost effective as it still uses shared environment without compromising security and accessibility. It also simplifies overall integration design, re-usability of provisioning services through template; streamline the usability and central monitoring solutioning for support team without compromising privacy or data or application level security. The key drivers for multi-tenant security design in cloud platform are:

- **Infrastructure** – Defines the platform setup and various patterns associated in defining the infrastructure components like storage, network, middleware, dependency handling to name a few. Many organization wishes to keep uniform Infrastructure principles in order to keep the risk and cost of handling to be low.
- **Security –** Defines the vital element of EA including Infrastructure or Platform security, Application security and Data security to comply with industry standards (HIPAA, SOC) and regulatory compliance to regional requirements.
- **Data** – Defines the data flow, operation of data handling in transaction, data structure, data integrity and low-level data flow operations.
- **Application** – Defines the actual technical stack of the application(s) to be developed as part of EA design, the interfacing components, the communication mechanism between application, dependency of different applications etc.,

2.2. Customer Identity Access Management

Customer Identity and Access Management (CIAM) enables application architecture to handle customer identity and profile data in a secured and flexible solution. There are many CIAM solutions available in the market and they have many commonality in terms of security, user management, profile management, policy management and more. CIAM is an integration of Identity, Security and Privacy of User data as shown below

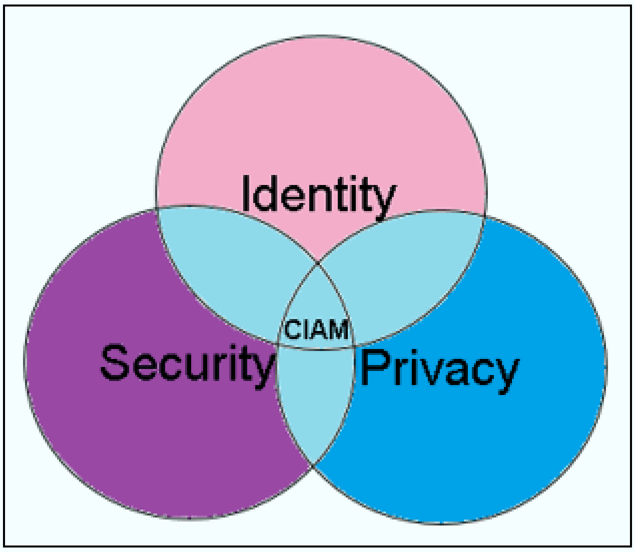

Figure 2: Customer Identity Access Management

Broadly, CIAM features are categorized as below:

Seamless customer experiences - Provide easy visualization solution during application integration and handle user access without much complexity.

Security requirements -Provide highest possible security for user data with a data store either integrated to CIAM solution or connected from CIAM application.

Performance and scalability - Handle any number of concurrency user access without trouble or delay in application access.

Privacy and regulatory compliance - With GDPR and customer personal data security in place for regulatory restrictions for different countries, CIAM plays an important role for monitoring, reporting and notification alert.

Adaptability - CIAM solution should have futuristic architecture to handle easy adoption for any architecture (Eg: Cloud Adoption, On-premises to Cloud synchronization etc.,)

2.3. Blockchain Based CIAM for Data Security

Blockchain is decentralized in nature and multiple participants of the blockchain platform can act as approver for the blockchain operation. For example, Data Security as a Service (DSaaS) implemented through CIAM can be operated through workflow operation using a Blockchain Smart contracts. This way, we can control data accessibility in a cloud platform using Blockchain based workflow operation. The layers which enables this DSaaS in cloud platform are listed below:

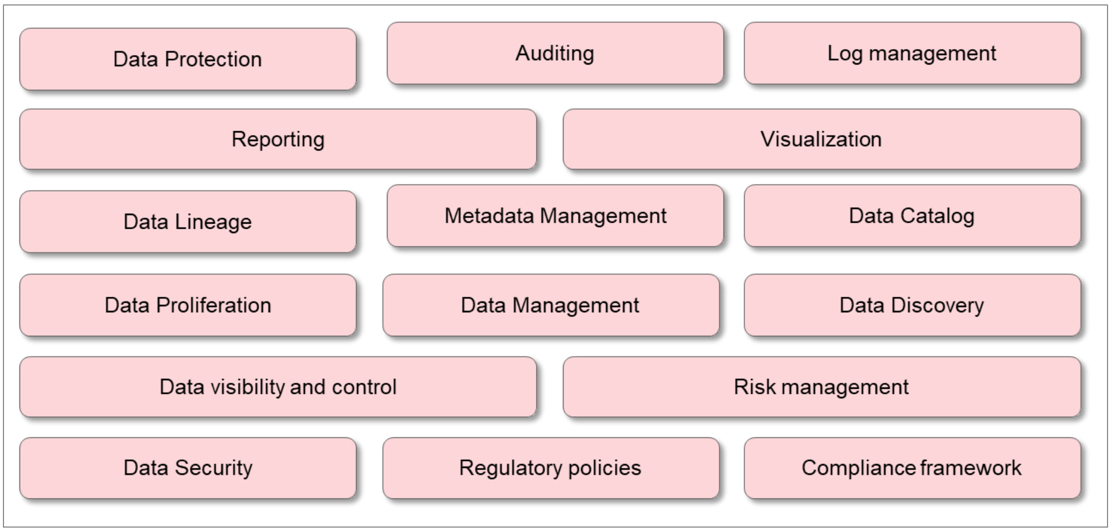

Figure 3: Component architecture for a Blockchain based DSaaS

Security Layer: This layer has the Smart contracts defined for the secured data transmission and data processing including application security, data security and interfacing security policies to be defined in the layer. This helps to ensure the complete network architecture is secured and role based access control is ensured in the service communication.

API Service Layer: This is the layer which exposes API services to external world in order to access the service interface for request handling, monitoring request, health check request to name a few.

3. EXAMPLE IMPLEMENTATION FOR DSAAS IN A DATALAKE ARCHITECTURE

Datalake is a classified pool of data in a Big data solution designed in a cloud platform for scalability and availability requirements. A set of data collection having relational information is called data puddle and a group of data puddle is called data pond. Multiple collection of data pond in a organization data is called data lake. Accessing data from a datalake should be protected from unauthorized access and different pond/puddle should be granted individual role based access to protect and isolate data security to the group of data.

A Datalake to protect from unauthorized access and isolate the data accessibility through workflow based approach is called De-identified Data lake (DIDL) and implementing DSaaS proves to be useful in such DIDL to improve performance and reliability to cloud platform solutions using Data lake services.

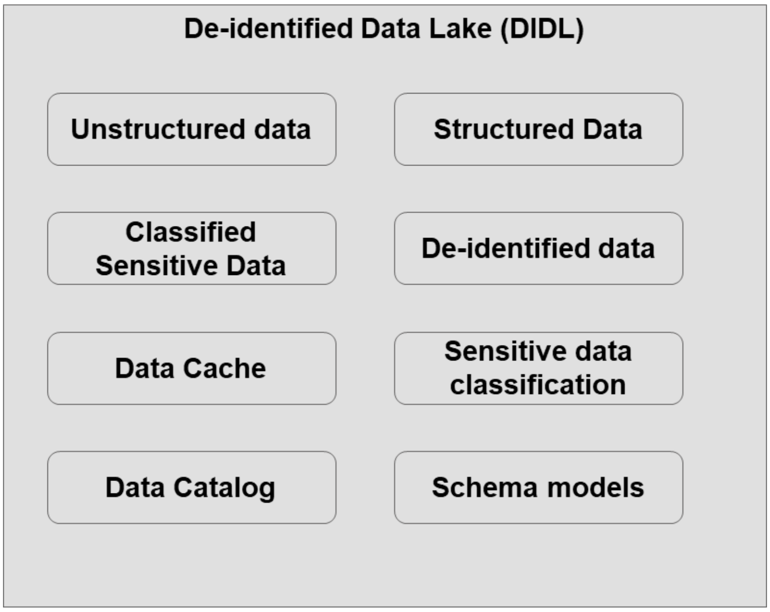

Figure 4: De-identified Data lake implementing DSaaS

DIDL is an architectural approach to protect data and handle risk governance in data privacy like PII protected data. It helps to discover, identify, monitor, catalog, query and protect data. It acts as a gateway keeper to Data Lake to remove identity of sensitive data before it moves in and out of Data Lake. The primary aim of DIDL is to create a data protection framework to secure, manage for compliance and cost effective data protection and risk management solution from Data Lake.

It has in-built Data catalog which monitors each and every asset in a Data Lake and also helps stewardship in data management to access data and provide role based data access. Also, for any Extract, Transform and Load (ETL) batch operation, it helps to add policy based data masking to enrich and store/manage protected data into the data lake.

In this context, conceptualizing Data Security as a Service (DSaaS), that provides various data security requirements, data security capabilities, services, policies, procedures, and associated use cases forms an important design consideration for any Enterprise. Key Components of DSaaS are shown in below Figure-5.

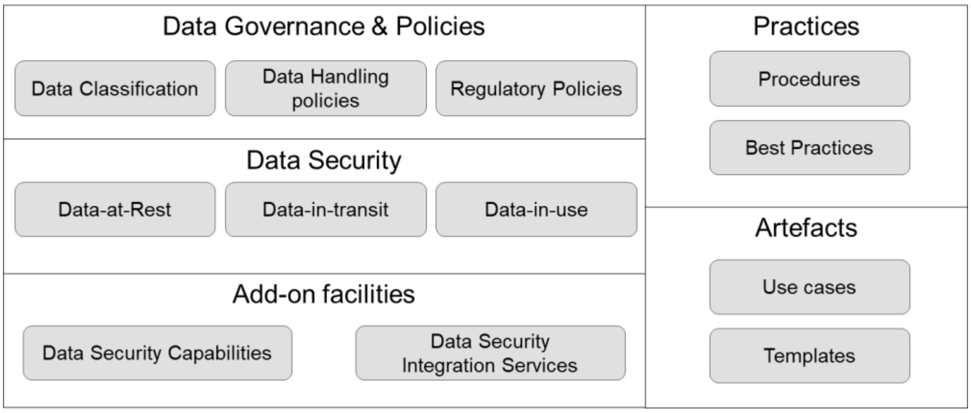

Figure 5: Key components of DSaaS

Blockchain platform can act as a main enabler for DSaaS in which a Distributed Ledger Technology providing an increased cyber resiliency and maintains ledger integrity because of its decentralized architecture, implementation of enhanced security frameworks for tamper-proof transaction, access patterns with no single point of failure (SPoF). The data is stored in blocks and connected with chain of blocks; thus, attacking a specific block does not affect the other blocks and the attacker needs to tamper all the blocks, but then detection is evident. The encryption and cryptography solution that Blockchain applications use to manage the data or transactions blocks protects individual transactions or records and the entire ledger. Thus, Blockchain proves to be a holistic capability to serve DSaaS requirements.

4. Reference Architecture of DSaaS

DSaaS (Data Security as a Service) architecture will comprise of all the components and services mentioned in previous section in a layered architecture. The services can be leveraged by any kind of solution irrespective of whether blockchain is used not. As shown in Figure-6, the DSaaS Architecture comprises of well-defined microservices and underlying components.

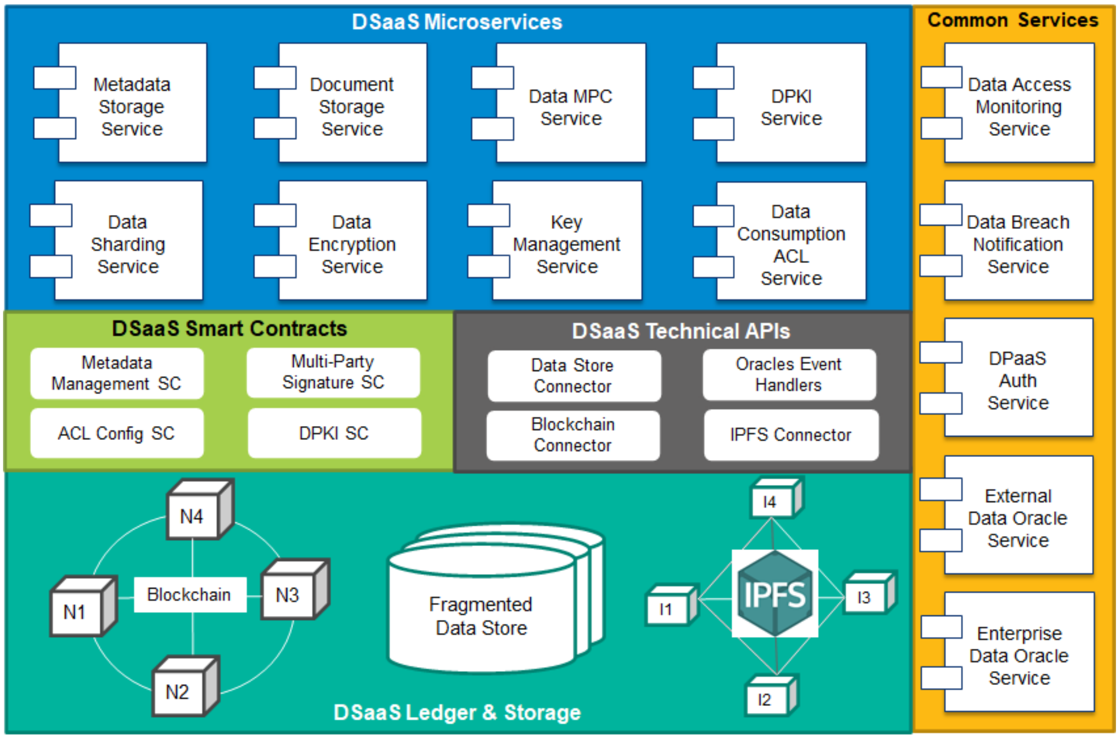

Figure 6: DSaaS Reference Architecture

Microservices architecture will be followed to build APIs with the right granularity and cohesive functionality and the components in the architecture are:

Metadata Storage Services: These are generic APIs which will provide ability to the client application to store metadata related to their assets and process in blockchain so that data protected at rest with complete provenance and audit trail. This can be used to store small sized data, or it can be used to store the reference and digital representation of large sized data or document

Document Management Service: For protecting large sized documents this API can be used to store the physical document on IPFS and its metadata stored on blockchain. Documents can either be uploaded as an attachment or a shared folder be specified for upload of very large documents.

Data Sharding Service: Highly sensitive large sized data and/or digital assets will be protected by using this API that performs data fragmentation and stores in an encrypted token form in the file system. The metadata and its associated access rights are maintained on blockchain using which the data is reconstructed by decoding and combining all fragments.

5. CONCLUSIONS

Data Security is the key to strengthen the Enterprise architecture when handling workflow operation involving multiple parties. For various industries like Fintech (Insurance, Payment, Investment banking) and Healthcare (EMR/EHR, Medical Retail Supplychain operations), it is important that an efficient pluggable DSaaS integration is incorporated which can help in business agility, cost efficiency and improved Governance and security compliance.

As shown in the reference architecture of DSaaS solution, there are many pluggable components which can be used to integrate a business agile solution for integrated Enterprise security to enable industry level compliance like FedRamp, PII, TOSCA, PCI or HIPAA compliance service functions.

ACKNOWLEDGEMENTS

The authors would like to thank Vinod Panicker, Hitarshi Buch and Krishna Mty from Wipro Limited in ideating and researching in the topic of Data Security as a Service using Blockchain platform and the joint idea is submitted as research paper in IBCOM 2021 conference.

REFERENCES

[1] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[2] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." 2012 International Conference on Computer Science and Electronics Engineering. Vol. 1. IEEE, 2012.

[3] Getov, Vladimir. "Security as a service in smart clouds--opportunities and concerns." 2012 IEEE 36th Annual Computer Software and Applications Conference. IEEE, 2012.

[4] Kumar, P. Ravi, P. Herbert Raj, and P. Jelciana. "Exploring data security issues and solutions in cloud computing." Procedia Computer Science 125 (2018): 691-697.

[5] Mohamed, Eman M., Hatem S. Abdelkader, and Sherif El-Etriby. "Enhanced data security model for cloud computing." 2012 8th International Conference on Informatics and Systems (INFOS). IEEE, 2012.

[6] Varadharajan, Vijay, and Udaya Tupakula. "Security as a service model for cloud environment." IEEE Transactions on network and Service management 11.1 (2014): 60-75.

[7] Hussain, Mohammed, and Hanady Abdulsalam. "SECaaS: security as a service for cloud-based applications." Proceedings of the Second Kuwait Conference on e-Services and e-Systems. 2011.

[8] Fernando, Yudi, Ramanathan RM Chidambaram, and Ika Sari Wahyuni-TD. "The impact of Big Data analytics and data security practices on service supply chain performance." Benchmarking: An International Journal (2018).

[9] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[10] Getov, Vladimir. "Security as a service in smart clouds--opportunities and concerns." 2012 IEEE 36th Annual Computer Software and Applications Conference. IEEE, 2012.

[11] Narula, Saakshi, and Arushi Jain. "Cloud computing security: Amazon web service." 2015 Fifth International Conference on Advanced Computing & Communication Technologies. ieee, 2015.

[12] Hussain, Mohammed, and Hanady Abdulsalam. "SECaaS: security as a service for cloud-based applications." Proceedings of the Second Kuwait Conference on e-Services and e-Systems. 2011.

[13] Kasthuri Magesh, Panicker Vinod, Buch Hitarshi and Mty Krishna "Data protection through data security-as-a-service using blockchain enabled platform" Proceedings of the Second International Conference on IoT, Blockchain and Cloud Computing (IBCOM 2021), Zurich Switzerland 2021.

AUTHORS

Dr. Magesh is a Distinguished Member of Technical Staff at Wipro. Magesh holds a Ph. D in Deep Learning and Genetic Algorithms. He is a senior member of IEEE and has published more than 50 articles in OpenSource For You, PC Quest, Cutter Business IT Journal and other notable international journals. He has also published around 480 thought leadership articles on AIML, Blockchain, and Cloud on LinkedIn with the hashtag #shorticle.