CALIFORNIA STATE UNIVERSITY, NORTHRIDGE

A Secure and Serverless Approach to Verification of Student Records

A graduate project submitted in partial fulfillment of the requirements

For the degree of Master of Science in Computer Science

By

Karandeep Singh Bhamra

May 2019

The thesis of Karandeep Singh Bhamra is approved:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Li Liu, Ph.D. Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Robert McIlhenny, Ph.D. Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Taehyung (George) Wang, Ph.D., Chair Date

California State University, Northridge

Acknowledgements

I am grateful to Dr. George Wang, for being my committee chair and giving me a chance to work on this project. In addition, I express my profound gratitude to Dr. Li Liu, and Dr. Robert McIlhenny for agreeing to be the additional members of my committee.

A special thanks goes out to my wife, Jessica, and my parents. The support my family provided me with went a long way in helping me finish this project in a timely manner.

Also, I would like to thank my friend Jesus Moran Perez, he was the one who initially inspired me with the idea for the project and has been of great assistance in helping me complete this project.

Table of Contents

Signature Page ii

Acknowledgements iii

List of Figures v

Abstract vi

Chapter 1: Introduction 1

Chapter 2: Related Work 5

Chapter 3: Serverless Architecture 6

3.1 Serverless History 6

3.2 Serverless Platform 11

References 13

List of Figures

Figure 1 – Virtual Machine 8

Figure 2 – Containerized Applications 9

Figure 3 – Event-based Functions 10

Figure 4 – Function Integration 11

Figure 5 – Serverless Platform 12

Abstract

A Secure and Serverless Approach to Verification of Student Records

By

Karandeep Singh Bhamra

Master of Science in Computer Science

Most academic institutions do not self-operate the system that is used for the verification of student records. Such a task is contracted out to firms who act as the middleman between the student and the potential employer who might be seeking verification of records. This project proposes a complete overhaul of that system and introduces a fast, and secure alternative system which accomplishes just that while maintaining low operating costs by making use of serverless architecture. The project consists of a scalable frontend website which is used to request a student’s record, the request is then processed by a web framework which routes it to an API endpoint where a serverless function retrieves the student’s record from a scalable database and generates a verified pdf certificate which is sent back to the frontend website client to be displayed. The project also implements tools for administering the blockchain like data structure that holds the student’s records and for verifying the integrity of the student records. The completed program demonstrates the entire workflow from the viewpoint of the client and the school administrator, while showcasing the benefits of implementing the system in a serverless architecture and how the student records are safe guarded against malicious modification.

**Chapter 1: Introduction**

Verifying a degree or any student record takes some amount of time, capital and patience. In addition, the verification process requires potential employers and background check firms to request confirmation of credentials from third party services associated with the academic institution rather than the institution directly. The results are not immediate and the privacy is implied, but not explicit. The data transaction should exist solely between the student, the institution and those that you want to share it with. A third party cannot be completely trusted to handle your private data. On the opposite spectrum, the student cannot be completely, trusted to provide accurate results, as the student providing it can manipulate it before delivering the modified records to those who requested it.

Since it has been established that verification of academic records takes time and money, most academic institutions have contracts with firms that provide the academic record verifications. There is unnecessary overhead related to that process; an employer or background check firm usually has to make a request with those middleman firms, who will then forward the request for records to the institution itself, or fetch the information from their own database which was provided to them [1]. I propose a solution in which the middleman can be cut out, and the verification process is provided directly by the academic institution. Overall, the main purpose of this project will be to create a proof of concept data storage format that borrows from and mirrors the blockchain data structure. In said data structure, the blockchain will hold a growing list of academic records of students, and will allow for the verification of the authenticity of those academic records. Once the format has been implemented, it will then be utilized to show how an academic institution can keep accurate and verifiable records relating to the students, and how a third party might be able to request and receive those records on an infinitely scalable serverless architecture.

Serverless architecture is a relatively modern concept. It is an application design where the business does not have to worry about managing the infrastructure that would support their application. In serverless architecture, there are still servers somewhere in the backend, however, the customer of those servers, is not responsible for managing them in any way. A person, business or any client would not have to worry about having to update the server, software, libraries, or be required to hire employees that would do the managing; instead, cloud providers such as Microsoft, Google, or Amazon, provide and manage the servers on your behalf, thus providing a seamless experience to the end client [2]. Serverless architecture relies heavily on event-driven programming, and executes code without provisioning servers through the use of functions. Functions are the pieces of code that make up the business logic, and they can be run within few milliseconds and the entire functions platform is provided as a service by most cloud vendors [3].

The term blockchain has taken off in popularity due to its connection to cryptocurrency. However, the data structure known as blockchain has many uses besides just cryptocurrency. A blockchain is a construct that acts as a digital database where the transactions are recorded in a secure and public manner. The concept can be simplified to this: anything can be owned, and there are things that we own and would like to share those items, and blockchains act as the middlemen which facilitate said exchange. A block refers to a specific record, or data that can be permanently recorded. A blockchain is a collection of those blocks appended one after another, and the blockchain acts as a historical record of all the total blocks added to date [4].

In a blockchain, the initial block is also known as the genesis block and is always hardcoded into the application. Once a block has been added to the blockchain, it is difficult to change that record [5]. The records are also verified by the network to make sure that they are valid before they are added to the blockchain. Each block also contains a unique code called a hash, and in addition, the current block also contains the hash of the previous block in the blockchain. A hash code is an output of a mathematical function, which is generally a string, that is composed up of series of characters and numbers. So, for a given unique input, the hash function will always yield the same hash; therefore, for someone to modify the blockchain, they will have to compute hash codes for each block and that is an extremely computationally intensive task depending on the underlying hash implementation. The benefit of a data structure like blockchain is that it is a digital log of all transactions that have occurred and due to its nature, it can be quickly searched and verified.

This project is organized in four distinct parts: serverless backend, the serverless frontend, serverless database, and an administrative student record software. The backend portion relates to the serverless computing provided via functions, which are ultimately responsible for providing the frontend client with the document that was verified and generated on the fly and transmitted over a secure communication channel. The frontend will be a website where the client enters the student information such as name and then the request is routed via a web framework to the corresponding serverless function and the received document is then displayed if the student record exists. The database is necessary for the storage of student records, the focus of the database will be on making it scalable, affordable and integrating the blockchain like data structure with the serverless functions, which when used in cryptocurrency, it is a decentralized system due to peer to peer network; however, for my project it will be a centralized system controlled by the institution due to an easier integration with the statefulness of the project. Lastly, since my project is a complete overhaul of how the records are handled now, it was necessary to showcase how an administrator in charge of this system would utilize it. The tool would allow a person in charge to load student records in a predefined file format, create a new student record, save the student record in the database, and verify the integrity of the records in the blockchain.

For a complete understanding of this project, it will be necessary to discuss other advancements in the area of using blockchains for academic institutions and related works, the underlying technology and algorithms used in serverless applications and blockchains. In addition, we will look at and compare the benefits of serverless versus other traditional architectures, a through comparison of the various cloud services providers, the implementation of the project and its subcomponents, the workflow of the whole system, the testability of the project and any further improvements that could have streamlined the whole operation if not for the for time or resource constraints.

**Chapter 2: Related Work**

As of the writing of this thesis, there are multiple corporations and startups that are starting to look towards blockchain to solve a host of problems. The storage and verification of data is a huge section of the outstanding problems left to be solved. Most recently, the popular hardware and software company IBM has partnered with Sony to make use of blockchain technology. IBM has created their own blockchain called IBM Blockchain, which will be the basis for a new platform geared towards academic institutions. Their goal is to allow students and schools to track each others progress. Additionally, such a system will make use of the built-in transparency and accountability due to it being based off of blockchain technology. According to IBM Japan, there are many preparatory schools based around Japan that have already incorporated IBM Blockchain along with student credentials to keep track of coursework and verify transcripts. A fully managed cloud service such as IBM Blockchain allows for institutions to rapidly adopt the technology without having to pay for new research and development for a private blockchain network.

Learning Machine is another small, private company which is hoping to make a big splash in the blockchain scene. Their goal is to provide a complete system to public and private bodies which will allow those parties to issue official, instantly verifiable records anywhere in the world. From the examples shown on their website, they issue verification for any type of company-wide or institution wide record. They have examples of an individual’s doctorate degree being verified and a certificate is issued with their information and the date their degree was conferred upon them. They intend to pioneer the way to allow businesses or schools to easily issue instantly verifiable records.

**Chapter 3: Serverless Architecture**

The tech industry is plagued with buzz words and new ideas that seem to be offshoots of old ideas. Most recently, “serverless computing” (also known as serverless architecture or function as a service, FaaS) is an application design pattern where cloud providers manage the infrastructure and your applications simply build and run on that infrastructure. At a glance, this is a great way to create and deploy applications. It allows for the client of the serverless architecture to focus on their business logic, without having to worry about the hardware, scaling and maintenance aspect of servers. The term serverless is however misleading. There are still servers, because otherwise it would hard for code to run on, but, the person or business that creating or deploying the application does not have to provision any servers personally.

**3.1 Serverless History**

Computers were not as powerful or portable as they are now. With the emergence of personal computers, much of computers moved away from the large, centralized mainframe systems to smaller client-server model. Early on when a client wanted to deploy an application, they would have to provision their own physical, bare metal server, install the required software tools, language frameworks, and any other dependencies of the application. In the beginning, all servers were bare-metal servers, which meant that each individual, physical server used by a single client. They would require a dedicated person of expertise whose sole job was to administer the server, and would be known as Server Administrators. The need for such a person was an additional cost for the client of the server, in addition to having to pay for any resources related to the cost of operation such as electricity, and other on-premise infrastructure costs. Eventually, with the development of virtualization, it became easier to rent out the server to multiple tenants. Now, a single machine could host multiple websites. Software and other web applications could be run on these virtual machines with completely different operating systems. It now became possible to run an application that depended on Linux operating system and at the same time run another application that depended on the Windows operating system. Even with virtualization there were still costs associated with it. The monetary costs dealt with any software or operating system licensing fees. Overall, virtualization led to a decrease in general costs due to the idea of multiple tenancy. A virtual machine could be created with specified number of virtual processors, dedicated memory and storage space; so, an application that required fewer resources would not be charged the costs associated with the higher resources. It became cheaper to run smaller applications rather than larger, resource hungry monolithic applications. One negative aspect of virtual computing would be that since the resources were divided among the various virtual machines, a larger, resource hungry application could easily starve out other applications. There are also issues with scalability, if your software becomes too large too quickly, the set, finite resources might struggle to keep up with the popularity. Bare metal servers and virtual machines still have their place in computing to this day and age, however, they did lead to newer, and improved ideas.

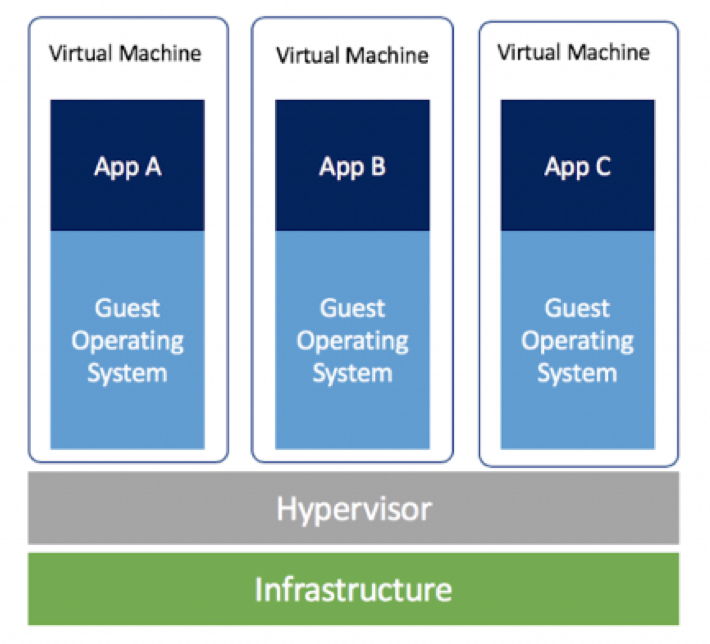


Figure [1] Virtual Machine

After virtualization, the next big idea was containerization. Application containerization is still a type of virtualization, but a container consists of an entire runtime environment. In essence, you are abstracting away the differences of various operating systems and hardware infrastructure, by bundling the application with all of its dependencies and files needed to run it into a single package. Docker is one of the most popular software that performs the operating system level virtualization. A single application can be packaged into a single docker container image which can be downloaded by anyone and installed on any operating system. It is now possible to run applications specific to a single operating system on any operating system platform that has the Docker software. Benefits of containers include consistency when shipping applications, you know the application will behave in a deterministic manner since it was tested and developed in a controlled environment. As popular as Docker is, it is not a one size fits all solution to computing. Some disadvantages of containers are that not all applications benefit from containerization, and there is a speed penalty when running a container. In virtualization or containerization, there is a performance overhead; containers are faster than virtual machines, but still not as fast as bare metal. Lastly, the data inside of a container is not persistent. Due to its design, the data generated when the container is spun up is lost when it is shut down, however, there are ways to save data from a container.

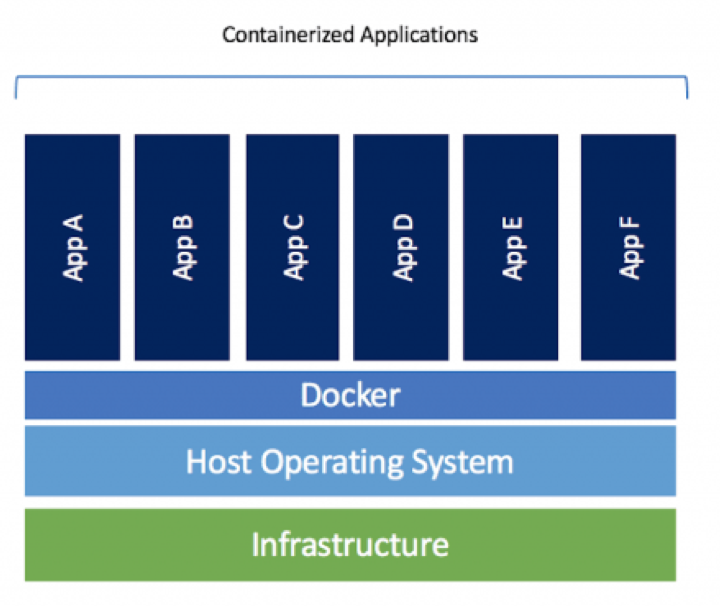


Figure 2 Containerized Applications

The latest fixation brings us to now, which is serverless computing via functions as a service. Functions are useful since they provide an on-demand functionality. Functions are a finite piece of code which are run when they are invoked. It is easy to become familiarized with functions since their underlying technology is based on containers. Functions are event-driven and are therefore invoked by any number of events, upon being invoked, the container where the code resides is spun up and the code is executed and the container is shut down. Therefore, you only pay for the amount of time your code took to execute and not for any of the underlying infrastructure. All function as a service provider also allow for easy and quick scalability of resources. When a function needs to scale up to meet a million requests or scale down to handle a single request, the cloud vendor handles all the underlying allocation and provisioning of resources. Since a function is just a program that will be executed, most vendors allow for programming in plethora of programming languages and have support for many of the popular frameworks. The usefulness of a function is defined by having it connect to various other cloud services such as databases.

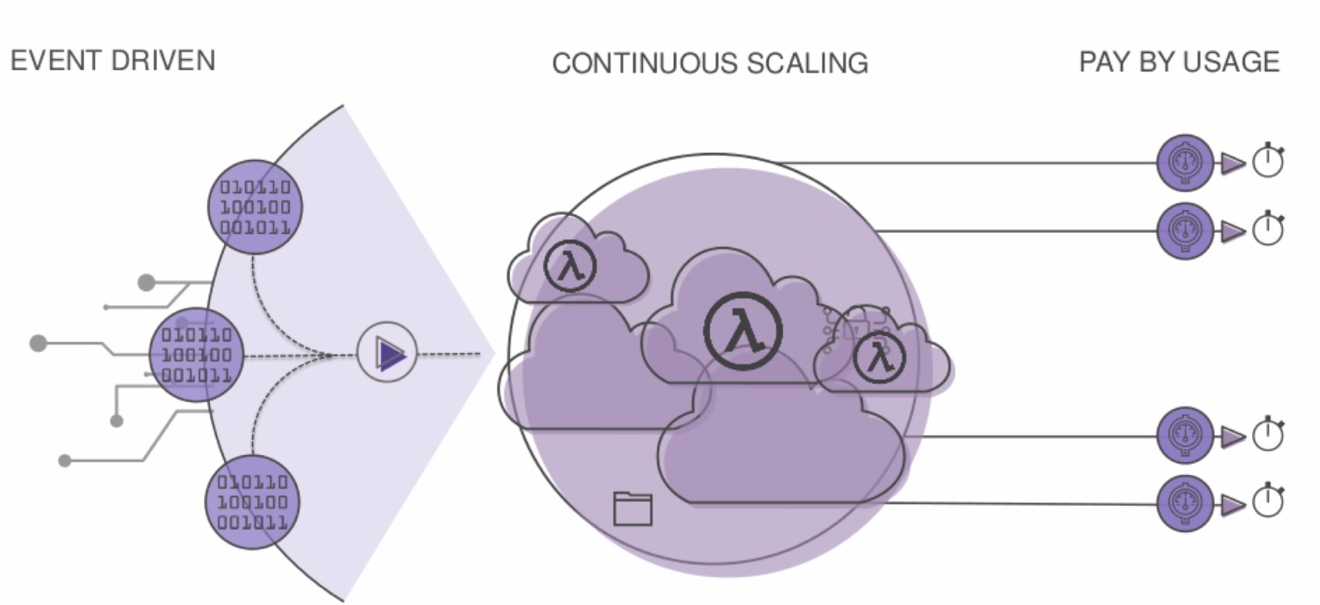


Figure 3 Event-Based Functions

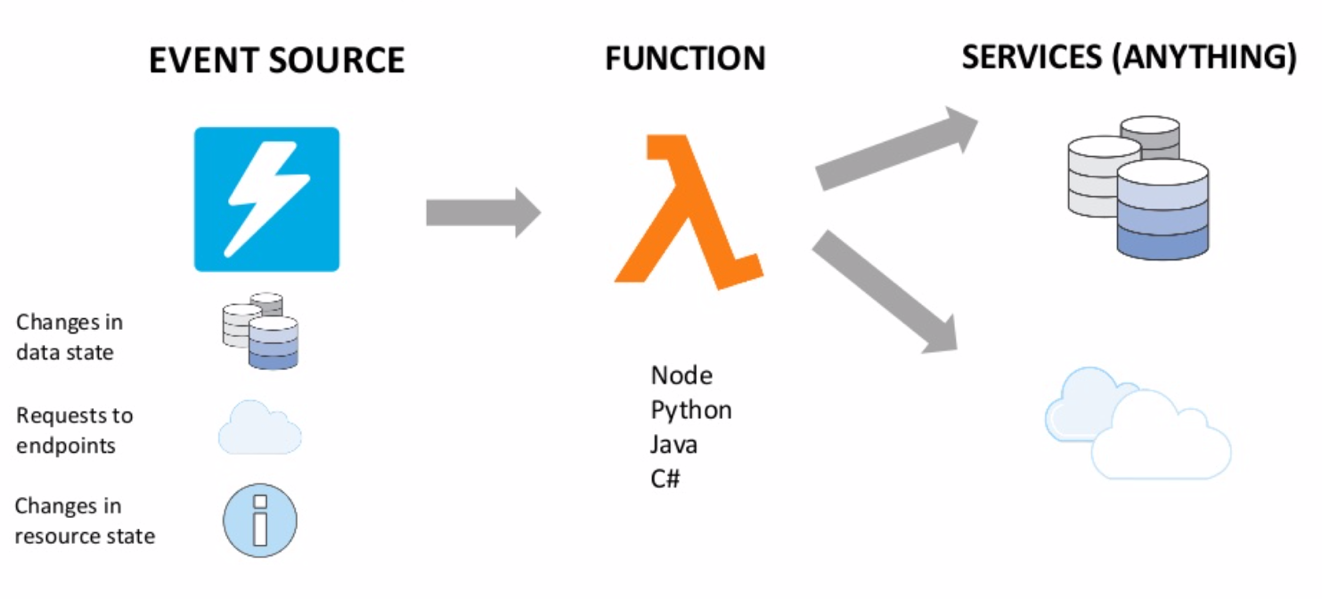
****

Figure 4 Function Integration

**3.2 Serverless Platform**

Functions are not the only cloud computing service that makes up a serverless architecture. As previously discussed, databases are also provided as a scalable service. Manually having to manage the capacity of a database can be time consuming; it is difficult to predict when there might be a spike of incoming or outgoing requests, so you have to be able to handle those requests dynamically. Many cloud services providers now have serverless databases that are simple, scalable, cost effective and highly available. Availability is one of the most important attributes associated with databases. If a database is unavailable, then the users of its data such as clients, and applications are unable to access it. Having an unavailable database is a detrimental to anyone relying on them. Due to the takeover of responsibility by the provider, developers and operators can save time and money by focusing on their business logic part of the application and less dependent on infrastructure support teams. In addition to databases, serverless platform also depends on managed services for API endpoints, message queueing service, continuous integration and continuous delivery pipelines, user management, and storage. Just about every important part of computing can be extracted to a managed service and offered to clients in an easy to use manner.

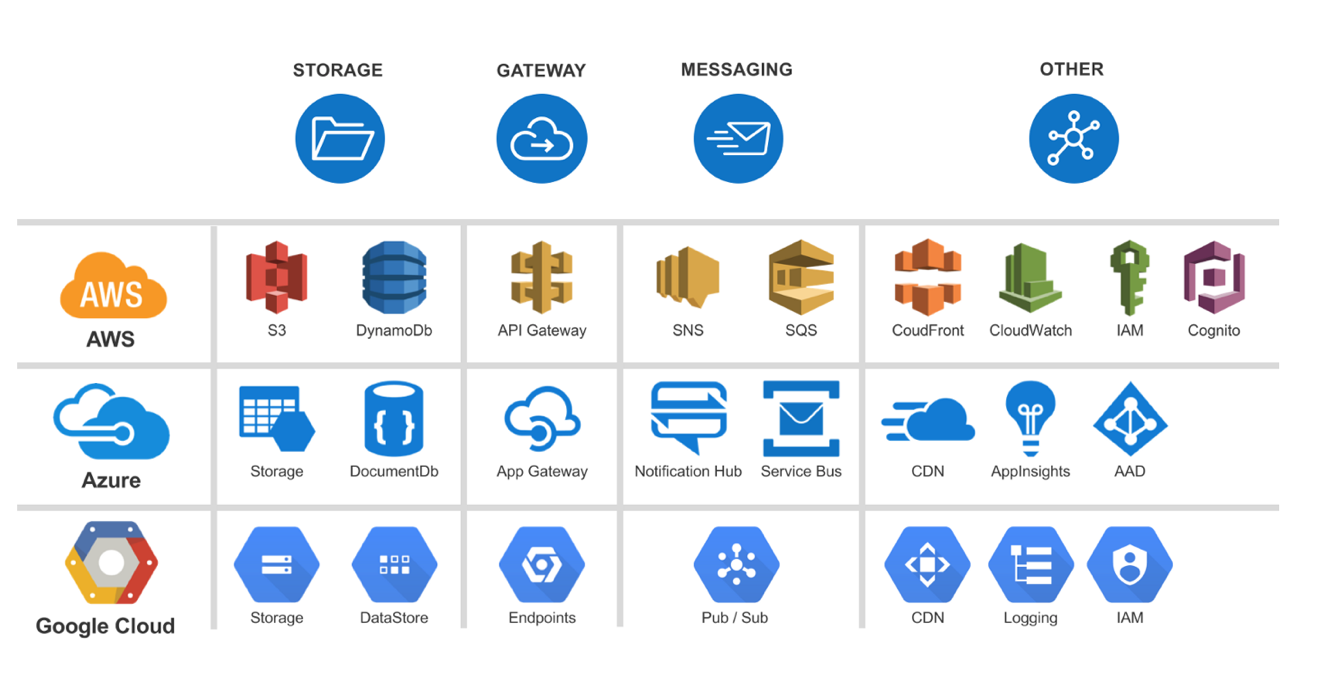


Figure 5 Serverless Platform

References

[1] Transcripts and Diplomas. (2017, July 13). Retrieved April 2, 2019, from http://www.csun.edu/alumni/transcripts-and-diplomas

[2] Nofer, M., Gomber, P., Hinz, O. et al. Bus Inf Syst Eng (2017) 59: 183. doi: 10.1007/s12599-017-0467-3

[3] Blockchain explained. (n.d.). Retrieved April 2, 2019, from https://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

[4] Fowler, M. (n.d.). Serverless Architectures. Retrieved April 2, 2019, from https://www.martinfowler.com/articles/serverless.html

[5] Bashir, F. (2018, May 28). What is Serverless Architecture? What are its Pros and Cons? Retrieved April 4, 2019, from https://hackernoon.com/what-is-serverless-architecture-what-are-its-pros-and-cons-cc4b804022e9