Auditoría de vulnerabilidades de seguridad de una arquitectura de procesamiento analítico basada en Azure ⋆

Beatriz P. de Gallo[1], Holman Bolívar[2] y Miguel Méndez-Garabetti[1]

[1] Laboratorio de Informática Forense (DigiLab), Instituto de Estudios Interdisciplinarios de Ingeniería (IEsIIng), Facultad de Ingeniería, Universidad Católica de Salta (UCASAL)
{bgallo,mamendez}@ucasal.edu.ar
https://digilab.ucasal.edu.ar/
[2] Grupo GISIC, Universidad Católica de Colombia
hdbolivar@ucatolica.edu.co

Abstract. Este trabajo aborda el estudio de la vulnerabilidad de la seguridad informática de la plataforma de servicios de cloud computing Microsoft Azure, considerando un conjunto de criterios críticos de seguridad. El estudio se focaliza en la definición de un plan de auditoría para identificar amenazas a los entornos de servicios de la nube, considerando como caso estudio la plataforma de estrategia analítica propuesta para el Grupo de Investigación en Software Inteligente y Convergencia Tecnológica (GISIC) de la Universidad Católica de Colombia. Se formulan las características fundamentales del plan de auditoría y se ejemplifican algunas de ellas para el caso de estudio.

Keywords: Auditoría · Vulnerabilidades · Seguridad Informática · Cloud Computing

1 Introducción

Según la Cloud Security Alliance (CSA) [2], durante los últimos años la computación en la nube se ha convertido en un componente neurálgico del desarrollo de nuevas tecnologías. La computación en la nube, o cloud computing, concepto con origen en las arquitecturas de software distribuidas [6], da soporte en la actualidad, a la mayoría de los servicios desplegados en internet.

Existen múltiples beneficios respecto a la adopción del cloud computing, pero seguramente una de las razones principales es la capacidad de escalar, mantener la flexibilidad y concentrar esfuerzos en las operaciones netamente distribuidas, sin la necesidad de administrar una infraestructura compleja. En este contexto, el presente trabajo aborda un estudio de vulnerabilidades de seguridad informática

⋆ Desarrollado por el Grupo de I+D+i de Forensia Digital de la Universidad Católica de Salta, dentro del proyecto "AED-BIGDATA: Aplicación de E-Discovery para el análisis forense de big data".

en la plataforma de servicios de cloud computing ofrecida por Microsoft Azure [7]. Para ello se considera el conjunto de 20 criterios de seguridad de la nube definidos por la CSA [1] y tomados por Sailakshmi [11], donde el autor lleva a cabo un análisis comparativo entre AWS, Azure y Google Cloud. Con el objetivo de identificar variables que permitan definir el grado de vulnerabilidad de una aplicación implementada en Azure, en este trabajo nos encontramos desarrollando una propuesta de plan de auditoría que permita validar dichas variables, así como alternativas de mejora en los casos que correspondan. A fin de validar el plan propuesto, se ha tomado como caso de estudio la arquitectura de procesamiento basada en Azure, definida para la estrategia analítica de datos del Grupo de Investigación en Software Inteligente y Convergencia Tecnológica (GISIC) de la Universidad Católica de Colombia. El trabajo presenta en la sección siguiente una descripción general de la problemática abordada, la Sección 3 describe el caso de estudio. A continuación, la Sección 4, presenta una breve descripción de los controles de seguridad utilizados y el plan de auditoría, y finalmente, en la Sección 5 se describen las conclusiones y el trabajo futuro.

2 Seguridad y Protección de Datos en los Servicios en la Nube

Son múltiples y conocidos los riesgos relativos a la privacidad y protección de los datos que deben afrontar los proveedores de servicios en la nube. Los usuarios de este tipo de servicios deben tener presente las políticas de privacidad definidas por los proveedores, ya que algunos incluyen la posibilidad de compartir información con terceros, además interesa conocer cómo se almacenan y cifran los datos, como es la gestión de acceso a usuarios habilitados, etc. Particularmente respecto de la privacidad de los datos, hay cuestiones legales pendientes, ya que, si no está explícitamente definido en las políticas del servicio, puede ocurrir que la propiedad de los datos quede sin establecerse con claridad, y brinda la posibilidad de que el proveedor del servicio pueda utilizarlos libremente. Respecto de este tema, la directiva 2002/58/CE del Parlamento Europeo [5] señala su preocupación por el resguardo de los datos personales y la privacidad de las personas. Siendo aún escasas las normativas legales instrumentadas a nivel internacional, salvo aquellas consideradas como requerimientos o recomendaciones que no tienen el peso legal como para incidir en los proveedores de estos servicios.

3 Caso de Estudio

Tal como se ha mencionado en la introducción, el caso de estudio utilizado en el presente trabajo se corresponde con la arquitectura de procesamiento de datos basada en los servicios de cloud computing de Microsoft Azure, del Grupo GISIC de la Universidad Católica de Colombia. Dicha arquitectura ha sido definida con el propósito de lograr modelos de estudio que permita el análisis forense de las herramientas de analítica de datos y vulnerabilidades de la seguridad de información que pudieran presentarse. El modelo propuesto de arquitectura de

solución ha sido diseñado teniendo en cuenta los requisitos de ingesta, procesamiento y análisis de datos de gran volumen y complejidad del proyecto en cuestión, los cuales exceden las capacidades de los sistemas de bases de datos tradicionales. En la Fig. 1 se presenta un esquema general de la arquitectura propuesta. Como se puede observar, la solución presenta una integración con diferentes orígenes de datos. Los datos de las operaciones de procesamiento por lotes se alojan en un almacenamiento de datos distribuido o data lake [8]. Donde se coloquen los mensajes entrantes para su procesamiento, la solución deberá considerar el procesamiento por lotes de los archivos de datos y además contar con instancias de procesamiento por flujo dependientes de los tipos de datos y sistemas de información involucrados.

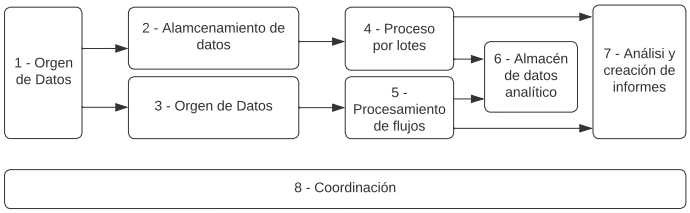

Fig. 1. Esquema general de la arquitectura propuesta.

Los datos de secuencias procesados se escriben entonces en un receptor de salida, se debe proporcionar un servicio de procesamiento de secuencias administrado, basado en consultas SQL de ejecución permanente que operen en secuencias sin enlazar, el procesamiento anterior confluirá después de la preparación de los datos. El almacén de datos analíticos que se utiliza para atender estas consultas y construir estos modelos se lleva a cabo utilizando el componente Azure Synapsis Analytics. También es posible que los datos se presenten a través de una tecnología NoSQL de baja latencia como HBase [13], o una base de datos de Hive [12] interactiva que proporciona una abstracción de metadatos.

4 Controles Críticos de Seguridad y Auditoría en la Nube

Los controles utilizados en este proyecto se basan en la matriz de control de la nube de la CSA, la cual divide estos controles en múltiples dominios: 1) Usuario de la nube, 2) Aplicación de la nube, 3) Integración de la nube, 4) Datos de la nube y 5) Procesos de la nube. Como se ha mencionado anteriormente, tales controles abordan los principales elementos de seguridad, clasificados como los 20 mejores por la CSA y que por motivos de espacio en este artículo no se listan en detalle, pero puede ampliarse en [1]. Por su parte, el proceso de auditoría de la seguridad informática de servicios de cloud computing está abundantemente

estudiado por Razaque [10], en el que discute acerca del rol del Auditor Externo en la tarea de control del nivel de seguridad de los servicios ofrecidos en la nube, y los problemas relacionados con la adopción de estas tecnologías que impactan en el grado de confianza de los usuarios finales. Teniendo en cuenta el alto nivel de confianza de los usuarios finales hacia los servicios de Azure, se tomará este enfoque como punto de partida para la auditoría de vulnerabilidades propuesta.

5 Plan de Auditoría

Esta sección comprende la definición del Plan de Auditoría para estudiar la vulnerabilidad de un entorno de cloud computing, identificar riesgos y establecer acciones de mejora posibles, considerando particularmente los criterios críticos de seguridad de servicios en la nube previamente identificados. Basada en la definición de Odio Gonzalez [9] sobre la auditoría de sistemas de información, se puede decir que la Auditoría Informática comprende la revisión, análisis y evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes, del entorno informático de una entidad, abarcando todas o algunas de sus áreas técnico-informáticas así como los procesos operativos vinculados a cualquier actividad que requiera de recursos tecnológicos informáticas y de comunicación para su ejecución. En este contexto un Plan de Auditoría incluye las definiciones necesarias para llevar a cabo esos procesos de revisión, análisis y evaluación de la infraestructura informática en toda su integralidad, y mínimamente, el Plan de Auditoría deberá incluir componentes de identificación de tareas, tiempos, recursos y responsabilidades, para cada actividad considerada en dicho plan. En los servicios de cloud computing, más allá de la solución tecnológica que puede ser más eficiente o menos eficiente dependiendo del caso en que se aplique, son fundamentales los criterios relativos a la privacidad y seguridad de los datos. Tan es así, que los usuarios definen su nivel de confianza en el proveedor del servicio, en función de las medidas de seguridad que ofrecen, principalmente, debido a que los servicios de este tipo carecen de regulaciones explícitas de seguridad y protección de la privacidad, y dependen de lo que cada proveedor formule desde su propio espacio. Por su parte, Odio Gonzalez [9] identifica ocho grupos de amenazas en los servicios IAAS: amenazas de requerimientos, de cumplimiento, de normativas, de arquitectura, de integridad de la información, de continuidad, de seguridad y relacionadas con el proveedor. Cualquiera sea el tipo de ataque que se produzca en los servicios en la nube (denegación de servicios, malware, Man-In-The-Middle, etc.) siempre se trata de eventos de acceso indebido, en el cual, el atacante descubre una boca de entrada, y una vez que esto ocurre, se exponen totalmente los contenidos en el espacio virtual considerado. Razaque [10] estudia particularmente el nivel de confianza del usuario ante el proveedor del servicio, y considera incluso la intencionalidad de los comentarios favorables o no que el usuario expone acerca del servicio que contrata, formando opinión que se transforman en comentarios de importancia para otros usuarios que analizan la incorporación de los servicios cloud para sus negocios. Por otra parte, también resulta de interés conocer el

grado de maduración del usuario respecto de la seguridad informática, identificando si la misma se encuentra incorporada en la cultura organizacional, y en qué medida está incorporada (nivel básico, medio o alto). Esto se puede analizar al relevar la arquitectura de seguridad informática existente en las instalaciones del usuario, identificando entre los aspectos más relevantes los siguientes: políticas de seguridad informática, creación de equipos de respuesta a incidentes de seguridad, gestión de riesgos, aplicación de normas relativas a la protección de datos personales (DIRECTIVA 95/46/CE [4] y 2002/58/CE [5] de la Unión Europea). Como última consideración sobre la auditoría informática, se debe incluir en esta discusión a las normas ISO/IEC 27000, que comprenden un conjunto de guías de acción y buenas prácticas relativas al desarrollo, implementación y gestión de los sistemas de gestión de seguridad de la información en las organizaciones. Estas normas, basadas en la mejora continua de la calidad, sirven de referencia práctica para las tareas de auditoría informática, y son plenamente reconocidas como tales. Se puede considerar el plan de auditoría atendiendo a dos enfoques críticos para el análisis de la seguridad en cloud computing: los factores técnicos de acceso indebido y los factores formales del contexto. A partir de estas consideraciones, se formula el Plan de Auditoria, cuyos principales componentes se enuncian a continuación.

5.1 Preparación de la Auditoría

En esta etapa inicial, el auditor deberá tomar contacto con la institución y su contexto, para comprender en toda su dimensión el modelo de negocio que se gestiona, así como las particularidades del caso. Por regla general, en esta etapa el auditor toma contacto con las políticas de seguridad institucional, realiza la revisión de auditorías previas si las hubiese y procede a entrevistar a personas claves de la organización. Para el caso particular de un análisis de seguridad en cloud computing, estas acciones deben particularizarse en:

- Aspectos de las políticas de seguridad institucional y documentos derivados de éstas que impactan de manera directa en los servicios de cloud computing.
- Revisión de auditorías previas de los servicios de cloud computing si los hubiere, y/o revisión de resultados de los procedimientos automáticos de monitorización de los servicios de cloud computing.
- Revisión de informes y conclusiones sobre incidentes de ciberseguridad si los hubiere.
- Entrevistas a quienes revisten responsabilidades en la gestión del modelo de seguridad planteado para la solución tecnológica.
- Revisión de documentos técnicos externos, que aborden aspectos relacionados con vulnerabilidades técnicas y/o niveles de confianza sobre el servicio de cloud computing.

5.2 Objetivos y alcance de la auditoría

Los objetivos que deben guiar la tarea del auditor se orientan a la verificación de la existencia y grado de cumplimiento de los controles previamente establecidos

en el modelo de seguridad establecido. El alcance de la actividad de auditoría deberá fijarse en los cinco espacios de seguridad planteados: 1) Usuario de la nube, 2) Aplicación de la nube, 3) Integración de la nube, 4) Datos de la nube y 5) Procesos de la nube. Para cada uno de estos espacios se debería definir el alcance en función del período de tiempo más adecuado (trimestral, semestral, a demanda, etc.) y de la profundidad de la actividad definida en función de la cantidad de eventos (o logs) que se requiere analizar.

5.3 Metodologías, técnicas y estrategias a utilizar

El desarrollo de la auditoría supone la definición del marco metodológico que permita cubrir todos los aspectos necesarios respecto del grado de cumplimiento del modelo de seguridad establecido. Los procedimientos que guiarán la revisión deben responder a los criterios de rigor respecto de los aspectos formales del procedimiento señalados por las normas de calidad como la ISO 27000, de la cual se pueden tomar ejemplos de cómo implementar los siguientes recursos:

- normativas sobre la confección de documentos,
- registro de hechos y dichos de los partícipes de la auditoría,
- definición de planillas de recolección de datos y registro de eventos que permitan recabar los datos técnicos correspondientes
- recolección de la evidencia según técnicas adecuadas para el tipo de dato que se quiere recoger
- cuando corresponda, prever la *revisión on line* de la plataforma tecnológica, con atención a la continuidad de aquellos procesos que no pueden ser detenidos, ya que el modelo de negocio exige el procesamiento continuo y sin interrupciones para determinadas funcionalidades del sistema.
- identificación y valoración de los riesgos inherentes al propio servicio de cloud computing, como aquellos resultantes de la interacción del sistema con el contexto.

Los cinco espacios de trabajo predefinidos deberán abordarse desde los dos enfoques señalados: los factores técnicos de acceso indebido y los factores formales del contexto. En el primer caso, será de mucha ayuda la recolección de la evidencia mediante la aplicación de herramientas forenses apropiadas y que permitan además el análisis estadístico y/o relacional de los datos recolectados para medir el grado de cumplimiento de los controles de seguridad establecidos, especialmente en casos de incidentes de ciberseguridad. En este caso, los riesgos a identificar son de tipo tecnológico usualmente, y se vinculan a las vulnerabilidades de los dispositivos y aplicaciones. En cuanto a los factores formales de contexto, el abordaje debe realizarse desde las entrevistas a las personas, sean éstas los usuarios finales, usuarios técnicos, responsables de la operatividad del servicio de cloud computing, referentes de los proveedores del servicio tercerizado si fuera el caso, responsables de seguridad informática institucionales, entre otros. Aquí tendrá mucho valor la experiencia del auditor en cuanto a sus competencias para tratar con las personas, ya que se trata de identificar el grado

de *cultura de la seguridad informática* presente en cada uno de los partícipes del sistema en análisis. En este caso, los riesgos son más complejos y difíciles de identificar debido a cuestiones propias del trato entre las personas y la cultura institucional.

5.4 Actividades del Plan de Auditoría

Considerando cada uno de estos componentes metodológicos y técnicos citados, el auditor deberá proceder a la formulación detallada del Plan de Auditoría, en términos de una definición de actividades, recursos y responsables para un horizonte temporal que también deberá definir según sea el caso. Cualquiera fuera el margen del espacio temporal de los recursos disponibles para cada actividad, el Plan de Auditoría debería contemplar una serie de actividades básicas detalladas (tareas, responsables, asignación de tiempos, asignación de recursos tecnológicos/económicos/logísticos) respecto de los dos focos de aplicación:

Acciones de acceso indebido:

- Selección de las herramientas forenses más adecuadas para la recolección de la evidencia de los incidentes de ciberseguridad si los hubo.
- Aplicación del análisis forense digital para la identificación de causas probables, origen, vectores de aplicación y otras variables de los incidentes de ciberseguridad si lo hubo.
- Análisis del contexto externo con datos actualizados acerca del nivel de confianza de la provisión de servicios de terceros.
- Entrevistas con el equipo de respuesta a incidentes de seguridad, especialmente si durante el período a analizar hubieran ocurrido incidentes de seguridad estén o no relacionados con el servicio de cloud computing.
- Selección e incorporación al equipo de auditoría de un responsable técnico para el desarrollo de tareas de pentesting para atacar el servicio de cloud computing con el objetivo de detectar y prevenir posibles fallos.
- Revisión de entornos de auditoría propios de las aplicaciones backend del servicio de cloud computing, y emisión de reportes de control de procesos ejecutados.
- Revisión de los registros de bitácora y/o agendas de eventos relacionados con la seguridad informática del servicio de cloud computing.
- Identificación y valoración de las vulnerabilidades de dispositivos y aplicaciones, y riesgos involucrados.

Factores formales del contexto:

- computing, identificando particularmente al:
  - Responsable de gestión y atención de usuarios en la nube,
  - Responsable de gestión de aplicaciones en la nube,
  - Responsable de gestión de integraciones en la nube,

  - Responsable de gestión de datos en la nube
  - Responsable de gestión de los procesos en la nube
- Obviamente cada uno de estos roles deben estar previamente identificados en las políticas de seguridad institucional y las normativas asociadas.
- Encuestas a diferentes usuarios según roles que cumplen en el servicio de cloud computing.
- Análisis del contexto interno acerca del nivel de confianza de la provisión de servicios de terceros.
- Medición de la eficacia, eficiencia y grado de impacto de las acciones de capacitación y generación de la cultura de la seguridad informática entre los diferentes usuarios del servicio de cloud computing.
- Revisión de las acciones de capacitación, concientización y generación de una cultura de la seguridad informática entre toda la comunidad usuaria del servicio de cloud computing.
- Identificación y valoración de las vulnerabilidades sostenidas en el comportamiento humano, e impacto en la seguridad del entorno.

En el marco de camino de la mejora continua, sería conveniente finalizar la auditoría con una definición de métricas, indicadores y variables de análisis sobre la documentación y resultados del proceso realizado, para la generación de un corpus de referencia que pueda medir desviaciones del estado actual frente al estado de futuros procesos de auditoría. Por último, un esfuerzo especial debe ponerse en el estudio de las vulnerabilidades encontradas, con el fin de estudiar cómo vencerlas, y del impacto que dichas vulnerabilidades producen en el servicio de cloud computing, para adelantar acciones tendientes a prevenir ataques automatizados.

Plan de Auditoría Aproximado para el caso de estudio Si se considera el caso de estudio definido en la sección 3, se puede bosquejar el plan de auditoría requerido para identificar las vulnerabilidades que pudieran estar presente en el servicio de cloud computing descripto. Los objetivos y el alcance de la auditoría se mantienen, y se organiza el plan de trabajo alrededor de los cinco espacios de seguridad planteados:

1. Usuario de la nube: ejemplificado con las áreas de salud pública de Colombia que recurren a esa web,
2. Aplicación de la nube: aplicaciones web del servicio de salud de Bogotá, Colombia (se pueden visualizar en https://saludata.saludcapital.gov.co).
3. Integración de la nube: plataforma Azure
4. Datos de la nube: DataLake basado en Azure Synapsis Analytic
5. Procesos de la nube: servicios de Virtual Machine de Azure.

Además de los componentes ya señalados para el marco metodológico de base, el caso de estudio debería contemplar:

- Planillas de recolección de datos para la interacción en entornos virtuales, ya que los partícipes del sistema no se encuentran todos ubicados en el mismo lugar y de manera simultánea.

- Herramientas automáticas de registro de las entrevistas con distintos tipos de usuarios
- Herramientas forenses específicas para la recolección de la evidencia en entornos de cloud computing, tales como Cellebrite UFED Cloud [3] u otros similares.

Por lo demás, las actividades detalladas del Plan de Auditoría para el caso de estudio deberían contemplar, además de lo dicho en carácter general, lo siguiente:

- Análisis del contexto externo con datos actualizados acerca del nivel de confianza de la provisión de servicios de terceros por parte de Azure.
- Entrevistas con el equipo de respuesta a incidentes de seguridad, especialmente si durante el período a analizar hubieran ocurrido incidentes de seguridad estén o no relacionados con el servicio de cloud computing.
- Selección e incorporación al equipo de auditoría de un responsable técnico para el desarrollo de tareas de pentesting para atacar el servicio de cloud computing con el objetivo de detectar y prevenir posibles fallos.
- Revisión de entornos de auditoría propios de Azure (Azure Policy).
- Entrevistas con los responsables del modelo de seguridad del servicio de cloud computing.
- Encuestas a diferentes usuarios según roles que cumplen en el servicio de cloud computing.
- Revisión de las acciones de capacitación, concientización y generación de una cultura de la seguridad informática entre toda la comunidad usuaria del servicio de cloud computing.

6 Conclusiones

Debido al incremento en la adopción de los servicios basados en cloud computing, y al incremento (en similar escala) en las vulnerabilidades a nivel de sistemas de información, el presente trabajo aborda el desarrollo de una propuesta de plan de auditoría que permita identificar el grado de vulnerabilidad en el despliegue de aplicaciones cloud native en la plataforma Azure. El abordaje se basa en un caso de estudio real, para el cual se han delineado las principales acciones de un plan de auditoría, que esperamos permita identificar de forma temprana posibles vulnerabilidades en estos espacios y de esta manera tomar medidas preventivas más que correctivas, respecto de los ataques a la ciberseguridad y respecto de la generación de una cultura de la ciberseguridad.

Referencias

1. Cloud Security Alliance, Top 20 Critical Controls for Cloud Enterprise Resource Planning (ERP) Customers (2019), https://cloudsecurityalliance.org/working-groups/enterprise-resource-planning/
2. Cloud Security Alliance (2022), https://cloudsecurityalliance.org/

3. Cellebrite: Cellebrite UFED CLOUD — Access Cloud-Based Evidence, https://cellebrite.com/en/ufed-cloud/
4. EUR-Lex: EUR-Lex - 31995L0046 - ES. Diario Oficial n° L 281 de 23/11/1995 p. 0031 - 0050;
5. Europeo, P.: Directiva 2002/58/CE del Parlamento Europeo y del Consejo. In: Diario Oficial de las Comunidades Europeas, p. 11 (2002)
6. Mell, P.M., Grance, T.: The NIST definition of cloud computing (2011). https://doi.org/10.6028/NIST.SP.800-145, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
7. Microsoft: Azure Proof of Concept Guide for Developers. Tech. rep., Microsoft Corporation (2020), https://clouddamcdnprodep.azureedge.net/gdc/gdcKySWnh/original
8. Nargesian, F., Zhu, E., Miller, R.J., Pu, K.Q., Arocena, P.C.: Data lake management. Proceedings of the VLDB Endowment **12**(12), 1986–1989 (aug 2019). https://doi.org/10.14778/3352063.3352116, https://dl.acm.org/doi/abs/10.14778/3352063.3352116
9. Odio González, C.: Desarrollo de un compendio de los contenidos regulatorios en Costa Rica y de gobierno de la seguridad de la información, con el fin de establecer una guía de auditoría para evaluar las amenazas técnicas sobre los servicios de cloud computing direccionados. Ph.D. thesis (2016), https://www.kerwa.ucr.ac.cr/handle/10669/27843 http://hdl.handle.net/10669/27843
10. Razaque, A., Frej, M.B.H., Alotaibi, B., Alotaibi, M.: Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey. Electronics 2021, Vol. 10, Page 2721 **10**(21), 2721 (nov 2021). https://doi.org/10.3390/ELECTRONICS10212721
11. Sailakshmi, V.: Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud (2021)
12. Thusoo, A., Sarma, J.S., Jain, N., Shao, Z., Chakka, P., Anthony, S., Liu, H., Wyckoff, P., Murthy, R.: Hive. Proceedings of the VLDB Endowment **2021-Spring**(236), 35–38 (aug 2009). https://doi.org/10.14778/1687553.1687609
13. Vora, M.N.: Hadoop-HBase for large-scale data. Proceedings of 2011 International Conference on Computer Science and Network Technology, ICCSNT 2011 **1**, 601–605 (2011). https://doi.org/10.1109/ICCSNT.2011.6182030