The latest security features of Microsoft Azure SQL Server Database

MET CS 674

Research Paper

Fariborz Norouzi

Fall 2018

Table of Contents

Table of Contents Figures

Abstract

Azure SQL Server Database is cloud- base relational database service based on SQL Server. It has some useful features that empower customers to secure and protect data. In this paper, briefly we will look different security layers including encrypting data, controlling and monitoring access in order to help us secure, and manage our cloud data and infrastructure. Also in continue, we will talk about some new features of Azure SQL Server database 2019 like integrated Azure SQL server Database with Hadoop Distributed Filing System (HDFS) and Apache Spark to handle big data job. Azure Machine learning workbench and python SDK platform are other cool tools of Microsoft Azure that become accessible to data scientists and developers.

Introduction

Azure SQL Server database is cloud- base relational database service based on SQL Server where supports enterprise grade security capabilities that customers can rely it. In Azure SQL Server database the security is defined in terms of layers, and it is called defense-in-depth. The first layer of security is how to protect the data itself, typically by using encryption. The second layer is how to control access, and finally the outer layer is how to monitor access.

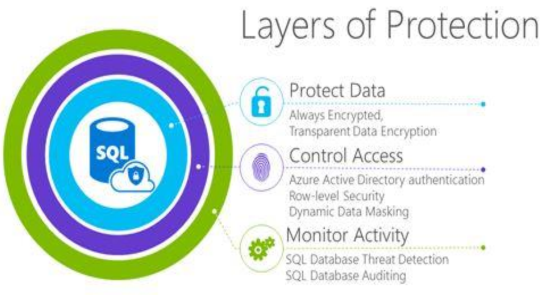

Fig1- Layers of protection in Azure SQL Server Database (Rengarajan, 2015)

Azure SQL Server Database has some useful features that empower customers to secure and protect data which the first innermost layer is about encrypting data that it’s protected data against different threats. For instance, encryption at rest is a very common requirement for customer who want to protect their data in case the file or disk are stolen. These features can be mentioned by varying degrees of granularity such as transparent data encryption, back up encryption and cell level encryption, which will be described in more detail in the following sections. The next level of security is about controlling access through authentication and authorization. Azure SQL Server database supports several features that enable to control access to data within the database itself.

Azure SQL Server has a very granular permission system allowing to control access to specific tables or even individual columns of data. It also supports active directory authentication which means enabling password-less single sign on using industry standard protocol. There are several programmability features to control which data can be accessed through the application layer such as row level security to control access to specific rows in a table based on querying user's role, or by enforce the masking policy to reduce the risk of accidental data exposure.

The third and outer layer of security is about monitoring access in order to keep track of who does and what, where, when and how they do it in database. Azure SQL Server supports a fine grained audit feature which allows us to specify which users' actions and objects should be tracked and then the database engine will log all activities based on tracking cases. This feature is commonly used by customers who an audit trail need in order to meet certain compliance standard. (Rengarajan, 2015)

Defense in-depth design of Azure SQL Database

Defense in-depth design of Azure services and capabilities to help us secure, manage, and monitor our cloud data and infrastructure. Microsoft designs and operates its cloud services with security at the core and provides us built-in controls and tools to meet our security needs. In addition, with machine learning Microsoft's significant investments in cyber defense, you can benefit from unique intelligence and proactive measures to protect you from threats. (Bahree, 2017) Azure offers unified security management and advanced threat protection for your resources, whether they're in the cloud, or data center, or even both. Services in Azure are built with security in mind from the ground up to host your infrastructure, apps, and data. All services are designed and operated to support multiple layers of defense, spanning your data, apps, virtual machines, network, perimeter, related policies, and of course physical security within your data centers. This includes how the data centers and systems that run. Azure are architecture and operated to the controls that you can leverage as part of your defense in depth security management. Everything start with identity and access control. (Ross, 2018)

Azure Server Roles and Logins

Security rolls are slightly different in an azure SQL server to those that we would find in a traditional on-premises SQL Server. In fact, there are only three server roles in an azure SQL Server. Firstly, there is the server level principal account and this is the account that creates the Azure SQL Server is equivalent to SA, but you can't call it. By SA, you are be able to reset the password to the account from within your portal like the security fix server role an on-premises instance of SQL Server. The login manager server role in Azure SQL Server has permission to create and drop logins. Therefore, only members are the login manager role or the server level principle login can drop and create logins. The DB manager role is similar to the DB creator server role for on-premises SQL instance. This can create and drop database and again only members of the DB manager role or the server level principle login can drop and create databases and they are the only three security roles available at the server level within Azure SQL Server. (Milener, 2017)

Azure Active Directory Authentication

All Azure resources are governed by Azure Active Directory. The control plan for security and access control is moving from the network layer to identify. That's why more of users are using Azure active directory (AD) not just for user sign-in, even for other things such as password management in the cloud group based assignments to applications publishing on-premises applications to the cloud conditional access policies and so on. With passing authentication, users get all of that but they get to keep their passwords on-premises. They don't need to leave their internal organizational boundary. It requires zero management with easy and free to use. It's secure, scalable and authentication.

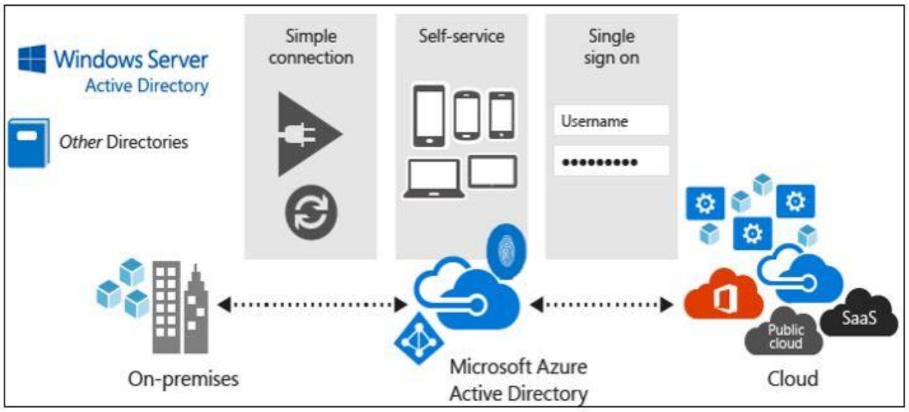

Fig2 – Azure Active Directory (Ross, 2018)

Azure AD always has a wide range of authentication options. Some of users use directory synchronization to sink just user names, but that means they have to manage separate passwords in the cloud. They also have password hash sync which lets they securely sync password hashes from on-premises to the cloud. In both these cases authentication happens in the cloud. If users want authentication to happen on-premises, their primary option is to use federation with ADFS (Active Directory Federation Services). But this needs additional infrastructure and network configuration on-prem. It works great if they are trying to support other diverse forms of authentication beyond password and third party multi factor authentication providers. (Rabeler, 2018)

If you want to manage password on-premises without implementation complexity then pass-through authentication is the best option for you. It gives you the full power of Azure AD cloud authentication and its full feature set. And lets you do it in a low-cost, secure and scalable way.

When you enter the username and password on the Azure AD sign-in page, server actually encrypts the password using a public key and then places the username and encrypted password on a queue for validation. One of your agent's on-perm makes an out band call from your network to retrieve the username and encrypted password. The agent decrypts the password using a private key that only it has access to it and tries to validate it against the on-premises active directory. Then the result of this which is returned by the domain controller. Success or failure is returned back to the agent which then forwards it up to Azure AD. Azure AD then decides what to do with it. If multi factor authentication is enabled, the user is challenged for it, if not the user just signed into the application. (Ross, 2018)

Transparent Data Encryption (TDE)

Transparent Data Encryption (TDE) is used to encrypt data files. This solves the compliance issue generally known as data as rest encryption. When Transparent Data Encryption database files are encrypted, prevents the data files from exploitation if data files were leaked. During the setup of SQL Server instance, the service master key is encrypted with Data Protection API DPAPI. And also Service Master Key encrypts the database master key on master database. By using database master key, a certificate on master database is created,

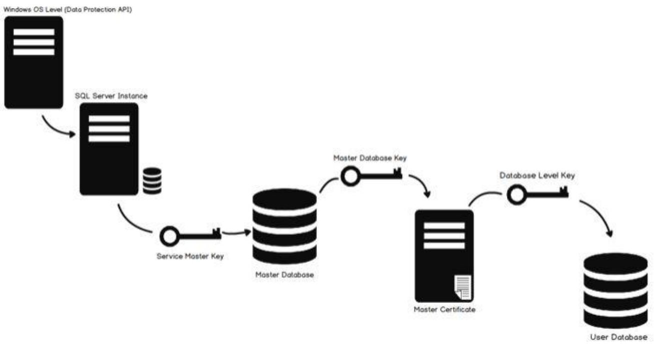

Fig3 - Using a certificate to enable encryption (Syed, 2016)

then the certificate on master database is used by all other databases on same instance to create Database Encryption Key (DEK). And in last step user database encrypts by the Database Encryption Key (DEK). (Syed, 2016)

Backup Encryption

Backup encryption is other new feature since SQL Server 2014 and it encrypts the data while creating a backup. Backup encryption uses encryption algorithms and a certificate or asymmetric key is used as an encryptor. (Ray, 2016) Performing an encrypted backup can be done by two ways. First way is encrypted backup to disk by access local disk or storage and second method is encrypted backup to windows azure storage by using the SQL Server backup to URL as the destination (cloud based)**.** The encryption steps for windows azure storage requires configure SQL Server credential to authentication to the Microsoft Azure by following steps: create SQL Server credential, create a database master key, create a backup certificate in the master database and finally by using the certificate and specify the encryption algorithm create backup the database.

Cell Level Encryption

Cell Level Encryption (CLE) uses inbuilt functions to perform to do encryption and decryption data with a symmetric key. (Mafli, 2017) In order to perform cell level encryption, you need permission to create a database master key which is a symmetric key for creating asymmetric keys and certificates for data encryption. The main advantage of CLE is encrypted data even when data loaded into memory and greater control over who access the keys along with high degree of customization, where enable user to configure it according the application requirements. (Arshad, 2014)

Azure Dynamic Data Masking (DDM)

Data masking divided into two basic flavors including static data masking and dynamic data masking. Static data masking (SDM) refers to permanently replaces sensitive data by altering data at rest, while Dynamic data masking (DDM) does to replace sensitive data in transit leaving the original at-rest data intact and unaltered. (Pomroy, 2017)

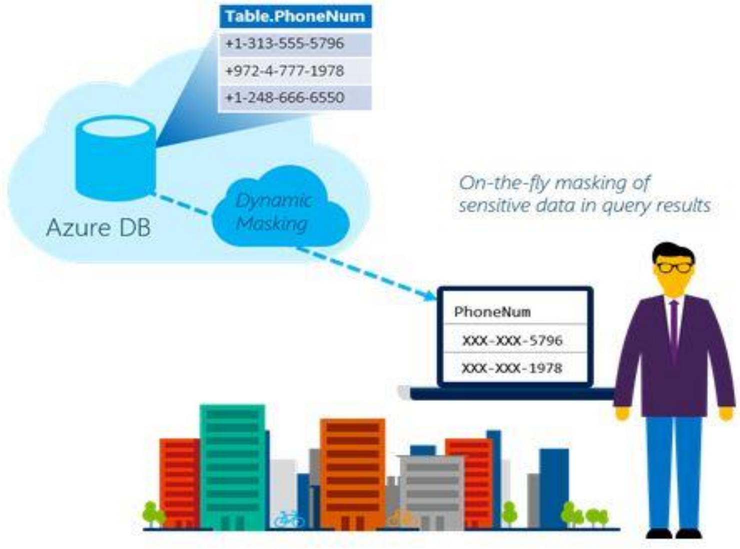

Fig4 – Dynamic Data Masking in Azure SQL Database (Reger, 2015)

Dynamic Data Masking (DDM) is intended to be a security feature instead of completely locking off access to all the data in a particular object. For less privileged users its owner can choose to show some of the sensitive data but not all of it in order to prevent the abuse of sensitive data by hiding it from users. Real time dynamic data masking eventually is a solution for data protection from internal and external threats. A threat can be something very minimal like your CRM user have the option to see sensitive information but the threat can be as well that an unauthorized source even internal source like developer that who should have access to this source of information. So SQL provides the option to enforce real-time dynamic data masking. The most important part understanding about real-time dynamic data masking is that the sensitive information never leaves the database and how exactly real-time dynamic data masking works with Azure SQL Server Database. Query generated by any application, then according to the policy a transformation function is injected to the query and sent to the database. The database is generating the mask information In Azure SQL Server database, multiple masking functions are available for various sensitive data categories like Credit Card number, Social Security number and so on. (Reger, 2015)

Azure SQL Database Auditing

One of the important tasks of a DBA is to be aware and to know what is happening on our server and our database. So this is just as true in the cloud as it is with our on-premises servers now as our SQL database offers two features which can help us with this. The first is called alert rules where we can create rules that will cause an email to be sent to an administrator when the rule has been breached and the second is the ability to create graphs of important metrics displayed in a dashboard so we can watch for trends and anomalies on our system. (Umansky, 2018)

Azure Security Center

One of the most important built in services is the Azure security center. Across Azure services, it provides unified visibility and control, adaptive threat protection, as well as intelligent threat detection and response. This gives you centralized and real-time monitoring into the security state of your Azure workloads with actionable recommendations and controls. Protection of data is often the core of our apps and services. Data protections are built for both structured and unstructured data. For structure data, all data is encrypted at rest, and machine learning can be used to proactively look for and alert you on potential security vulnerabilities. These can be related to data encryption, enabling security telemetry, and extend to capabilities in data services themselves to recommend and enable sensitive information discovery and classification, dynamic data masks to obscure data fields and more. Database services in Azure can be configured to run these checks automatically, and Azure's security center will alter you on any potential issues it finds to keep your data protected. (Bahree, 2017) For unstructured data, storage accounts span also encrypted at rest, by default, and each account is geo-redundant. Users can also apply further protection using access keys to control authentication, shared access signatures for secure delegated access, and granular

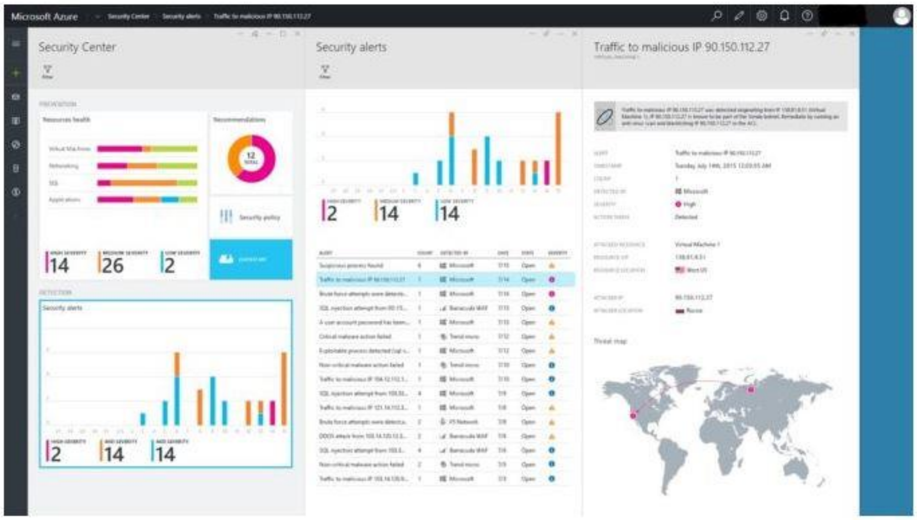

Fig5 – New Azure Security Center (Bahree, 2017)

network firewall controls. Azure security center will report its findings when security is at risk, or when protections have been disabled by an admin. Now apps are the front end for accessing and presenting data and their security's generally governed through data, VMs, or computer platform services in Azure. Your web apps can be configured to use Azure managed service identities to streamline secure communication with other services connected to Azure AD. You can manage SSL certificates for your apps and even require the clients connecting to your apps have valid certificates for inbound requests. Now as you move into VMs and compute, the Azure security center uses machine learning to continuously access security and vulnerability levels of your VMs, networks and service configuration. It also gives your actionable recommendations to prevent exploits before they occur and dynamically applies allow and block lists to keep out unwanted traffic. Users can also benefit from intelligent threat detection and response. The security center leverages a Microsoft intelligent security graph to discover and take actions against attacks. Microsoft collects across all of its services and industry data to block known attack patterns. Azure also gives you the control that you need to prioritize alerts and incidents that are important to you. In addition, Azure studio gives you a unified view for forensics analysis and the ability to search across all of your computer resources. You can even visualize threat intelligence down to the trending attack techniques and the geographic regions affected. (Karlin, 2018)

For network security, the Azure security center will assess and report on potential network and security issues related to open ports and firewall settings, and network security groups. Azure provides additional security when designing and architecting user apps to enforce logical network boundaries and limit permissions to network security groups. Users can also control network and other resources, like VMs, just in time controls for opening management and internet ports, with intelligent recommendations to reduce exposure to brute force attacks.

Azure DDoS Protection

Beyond your network controls, the perimeter security, Azure’s DDoS Protection for protection against Distributed Denial of Service attacks is available at a basic level by default. Azure’s DDoS Protection Standard version and mitigations against volumetric attacks, where the attacker’s goal is to flood the network with traffic, in efforts to disable your services. (Dial, 2018) Protocol Attacks where the attackers tries to find and layer for protocol stacks. Application layer attacks, where the web application packets are used to disrupt transmission of data between hosts, like cross site scripting or HTTP protocol violations.

Fig6 - DDoS Protection Standard features (Dial, 2018)

For security policies and access management, Azure has a comprehensive set of services to securely manage security policies and access to resources, whether accessed by people or programmatically by your code. These controls are more than just your front door to who or which processes can access your apps files or data and extends how granular access is delegated to your IT and development team, using role based access controls to ensure your team member only have access to what they need.

To automate the response to specific security events, you can also use a security playbook. Powered by logic App, which is used in Azure to automate workflows, this orchestrates the set of actions that need to happen when a predefined event is detected by the Azure security center. Beyond the policies that you can set, security’s infused in everything we do as we develop Azure’s services. All the way to development delivery, using the secure development lifecycle process. Fabric admins operate Azure’s services with zero standing privilege, and use just in time approval processes to gain temporary access to sensitive data or controls when needed. Azure services compile with both international and industry specific compliance standards and are subject to rigorous third party audits that verify Azure security controls.

Azure Physical Security

Finally Azure extends its layered approach to physical security. Data centers managed by Microsoft have extensive layers of protection. Access approval of the facility's perimeter, the building's perimeter, inside the building, and on the data center floor. This layered approach reduces the risk of unauthorized users getting physical access to data on the data center resources. (Lanfear, 2018)

So that was the primary defense and security considerations in Azure, at every defense in-depth layer. These controls are all part of a shared responsibility model in Azure, comprising the security Microsoft manages as the service provider, built in controls for you and the intelligence Microsoft can provide you from its global scale cyber defense operations.

New Features of Azure SQL Server Database 2019

Azure SQL Server Database 2019 product offering a cross platform multi database tools designed to empower data engineers and data scientists.

Azure SQL Server 2019 is providing the flexibility to run on the cloud. It provides a unified view over enterprise data. Whether its relational data stored in database or big data stored in high distributed file system (HDFS) clusters. Azure SQL Server 2019 allows querying data from other data sources such as Oracle, MongoDB, and Teradata. (Brust, 2018)

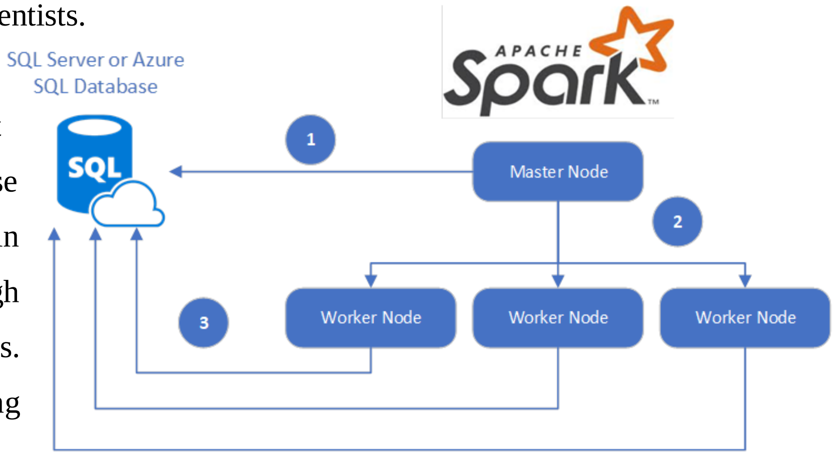

Fig7 - Big data analytics with Spark connector for Microsoft SQL Databases (Wu, 2018)

Data visualization provides data quality, data security and data privacy. In Azure SQL Server Database 2019, there are the ability for the SQL engine to read files located in the Spark HDFS. Once user create the external table over the files in HDFS, SQL Server joins high value data in relational database with high volume of data in HDFS. It also provides scalable compute and storage for faster data processing. Both SQL and Apache Spark together provide query capabilities over scalable storage across relational and big data. By Azure Data studio you can easily brows your files in HDFS and in one click you can start analyzing your files in a notebook. (Brust, 2018) By Azure SQL Server 2019, you can create a single virtual data layer that's accessible to nearly every application. Poly based data virtualization handles the complexity of integrating all your data sources and formats without requiring you to replicate or move it. You can streamline data management using Azure SQL Server big data clusters deployed in kubernetes every node of a big data cluster includes SQL Server relational engine HDFS storage and spark which allow you to store and manage your data by using the tools of your choice.

Data scientists spend a lot of their time to prepare the data. In Azure data studio, data scientists are more productive. With Azure data studio, you have an integrated notebook viewer which seamlessly connects to the SQL Server 2019 cluster. The notebooks allow customers to install customers AI and ML packages including rates, visualization and libraries. It's attached to the PI Spark kernel and lets you submit your spark jobs against the cluster. You can build a rich spark job graph viewer which would allow you to monitor your submitted spark job.

Conclusion

Growing volumes of data, create deep pools of opportunity for those who can navigate it by Azure SQL Server database to stay ahead of making data integration management and secure intelligence easier with more intuitive than even before. Azure makes it easier to build intelligent apps with big data. Also you can run spark jobs to analyze structured and unstructured data train models over data from anywhere with SQL Server machine learning services. From security perspective, Azure security center provides new services that help users tap into Microsoft's real-time intelligence on the threat landscape, including how it can help users get centralized security monitoring, set policy and deploy security controls for their Azure resources. It also get advanced threat detection with machine learning. Azure data studio provides a seamless experience over the data.

References

1- Rengarajan T. K. (2015), Microsoft Azure SQL Database provides unparalleled data security in the cloud with always encrypted. Retrieved from: https://azure.microsoft.com/en-us/blog/microsoft-azure-sql-database-provides-unparalleled-data-security-in-the-cloud-with-always-encrypted/

2- Bahree A. (2015). New Azure Security Center Enhancements. Retrieved from: http://azurepost.com/new-azure-security-center-enhancements/

3- Ross E. (2018). What are the fundamentals of Azure identity and access management? Retrieved from: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-fundamentals

4-Milener G. (2017). Server-Level Roles. Retrieved from: https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/server-level-roles?view=sql-server-2017

5- Rabeler C. (2018). Use Azure Active Directory Authentication for authentication with SQL. Retrieved from: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication

6- Ross E. (2018). What is Azure Active Directory? Retrieved from: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

7- Syed A. (2016). How to configure Transparent Data Encryption (TDE) in SQL Server. Retrieved from: https://www.sqlshack.com/how-to-configure-transparent-data-encryption-tde-in-sql-server/

8- Ray M. (2016). Create an Encrypted Backup. Retrieved from: https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-an-encrypted-backup?view=sql-server-2017

9- Arshad A. (2014). Granular or Cell Level Encryption in SQL Server. Retrieved from: https://www.databasejournal.com/features/mssql/granular-or-cell-level-encryption-in-sql-server.html

10- Mafli K. (2017). SQL Server TDE vs Cell-Level Encryption: A Brief Comparison. Retrieved from: https://info.townsendsecurity.com/sql-server-tde-vs-cell-level-encryption-a-brief-comparison

11- Reger R. (2015). Dynamic Data Masking is now generally available for Azure SQL Database. Retrieved from: https://azure.microsoft.com/en-us/blog/dynamic-data-masking-generally-available/

12- Pomroy S. (2017). Static vs Dynamic Data Masking. Retrieved from: https://www.imperva.com/blog/2017/07/static-versus-dynamic-data-masking/

13- Umansky A. (2018). Get started with SQL database auditing. Retrieved from: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing

14- Lanfear T. (2018). What is Azure Security Center? Retrieved from: https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

15- Dial J. (2018). Azure DDoS Protection Standard overview. Retrieved from: https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview

16- Lanfear T. (2018). Azure facilities, premises, and physical security. Retrieved from: https://docs.microsoft.com/en-us/azure/security/azure-physical-security

17- Brust A. (2018). The big data odyssey of SQL Server 2019, and more data and AI news from Microsoft Ignite. Retrieved from: https://www.zdnet.com/article/data-and-ai-news-abounds-at-microsoft-ignite/

18- Wu X. (2018). Accelerate real-time big data analytics with Spark connector for Microsoft SQL Databases. Retrieved from: https://azure.microsoft.com/en-us/blog/accelerate-data-analytics-with-spark-connector-for-azure-sql-database-sql-server/