Threat Modeling Stapes to Mitigate Could Threat

Md Haris Uddin Shairf [#1], Ripon Datta [*2], Shaamim Udding Ahmed [#3]

[#] *University of the Cumberlands, United States of America*

Abstract *— The purpose of this work is to identify the various steps used in the threat modelling process. This paper, therefore, seeks to explain the assets implemented in facilitation of the process, the architecture used, the data required, along with how it is utilized, and identification of the threats. Another objective of this work is to identify how severe the security threats are. Primary and secondary data sources are analyzed. Also, a review of literature is done to provide more insights and information that supports or helps meeting the herein presented objectives. A step-by-step process of threat modelling is identified which include identification of security objectives; identification of assets and external dependencies; identification of trust zones; identification of potential threats and vulnerabilities; and documentation of threat model. Analysis the common global threats based on cloud data breach. We also analysis few threat models that can be the number of solutions to consider. The key to this paper is to present a valid asset and walk through the threat modelling process, find a better threat modelling scope.*

Keywords — *Authentication, Biometrics, Security Analysis, Biometrics-technique, Access Control.*

I. INTRODUCTION

Security threat demonstrating, or threat displaying, is a procedure of evaluating and recording a framework's security dangers. Security risk demonstrating empowers you to comprehend a framework's danger profile by looking at it through the eyes of your potential enemies. With procedures, for example, section point recognizable proof, benefit limits and danger trees, you can distinguish methodologies to relieve potential dangers to your framework. Your security risk displaying endeavours likewise empower your group to legitimize security includes inside a framework, or security rehearses for utilizing the framework, for ensuring your corporate resources. Physical Controls of e-commerce industry has been an area dealing with significant volume of threats and loss in terms of assets and equipment. [11].

II. IDENTIFY THE ASSETS

Microsoft Azure cloud system is most the well known disseminated distributed computing stockpiling framework. Advancement Company Microsoft manufactured the capacity framework for putting away information, records, send, oversee, and fabricate web-based applications. Azure services are overseen through an overall system framework that Microsoft worked by utilizing their server farms. Worldwide appropriated clients can utilize the Azure service to oversee different web-based applications. The Azure entrance empowers customers/clients to peruse productive assets, dispatch new assets, adjust settings, and see the fundamental checking data from dynamic virtual service and machines [1]. Microsoft cloud service is prominent for all sort of organization due to the Azure Cloud Services. It is the best example of the platform as a service

(PaaS). The innovation (Azure App Service) is intended to help electronic applications to be increasingly versatile, dependable, and modest to work. Microsoft cloud has committed facilitating assets; Azure Cloud service has around 700 administrations accessible. Here are the few Azure cloud base administration model Azure App Service, Azure Virtual Machines, Azure DevOps Project, Pay-as-you-go Azure Backup, Cosmos DB, Azure Active Directory, Azure Kubernetes Service [2]. Microsoft on its most recent quarter uncovered its business cloud income and a yearly run rate north of $21 billion [3]. Figure 1 demonstrates the top income kept running by Microsoft, and the second position is in Amazon.

Cloud vendor	Annual revenue run rate
Microsoft commercial cloud	$21.2 billion
Amazon Web Services	$20.4 billion
IBM	$10.3 billion
Oracle	$6.08 billion
Google Cloud Platform/G Suite	$4 billion
Alibaba	$2.2 billion

Figure 1: Source: Company filings, earnings reports [3].

III. ARCHITECTURE

Azure Active Directory Technical Architecture Figure 02 [4]. Microsoft has a great deal of material distributed about Azure AD. However practically none of it is designed in nature, and what is compositional is centred on a particular segment. Consequently, it is hard to conceptualize the master plan of what Azure AD is actually and how

everything associates. Microsoft made a general engineering architecture to help give that setting to Azure AD [4].

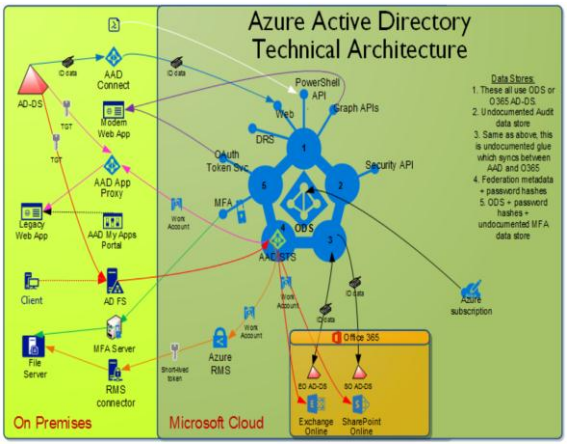

Figure 2: Azure Active Directory Technical Architecture [4].

Figure 02 explains. Azure AD has many segments, interfaces, and information stores–definitely more than its on-premises partner AD-DS. This chart (Figure 02) indicates most yet not these parts. Personality information streams along the blue line to AAD from AD-DS through AAD Connect. It additionally streams along the dark line to Office 365 applications (and from Exchange Online). It can, on the other hand, stream to AAD utilizing the Power Shell API or Graph APIs. Verification streams to the Azure AD STS along the red line through ADFS. ADFS uses AD-DS as an authenticator. The outcomes in a Work Account token, which is passed to different applications utilizing AAD like Office 365. Heritage web applications can uncover a higher security customer endpoint in the cloud using AAD App Proxy. A Work Account token is acquired, and the AAD App Proxy connector brings an AD-DS token. The heritage web application doesn't have to comprehend AAD by any stretch of the imagination, and any customer that can reach AAD can get to the web application. Current web applications influence the Graph APIs to get character information and the OAuth token support of gain admittance to other present-day web applications. Document servers can use Azure MFA through an on-premises MFA server. They can likewise use Azure RMS employing an on-premises RMS connector. Cloud administrations upgrade the security of on-premises administrations. Your Azure subscription(s) are homed in your AAD inhabitant, giving character administrations to your cloud-based Azure administrations [4].

IV. AZURE DATA FACTORY PROCESS

Azure Data Factory provides a key contribution to Modern Data warehouse scene since it coordinates effectively with unstructured and structured information, whether on-premises or in the cloud. All the more as of late, it is starting to incorporate remarkably well with Azure Data Lake Gen 2 and Azure Data Bricks too. The chart beneath works admirably of delineating where Azure Data Factory fits in the Modern Data warehouse scene. As should be evident from this chart, Data Factory is essential between source, destination, and explanatory frameworks. Also, by including a code-free graphical client-based interface, for example, Mapping Data Flow that uses Spark groups in the cluster, Azure Data Factory is sure to assume an essential job in the plan and improvement of the Modern Data warehouse [5]. The data flow involves On-Premise data source selection, Azure Data Factory, Azure Data Lake Store, Azure Data Bricks all those can interact with Azure SQL, Cosmos Database. Also, all those services can be represented by using Power BI tools.

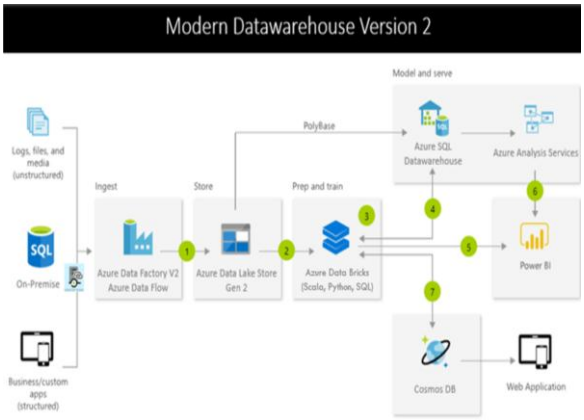

Figure 3: Azure Data Factory [5].

V. IDENTIFIES THREATS

In the efforts to achieve efficient and effective neutralization of threats as well as reduction of false positives, firms collect and carry out analysis of log data from the Azure resources, where the network along with third-party solutions such as firewalls and endpoint solutions are implemented. Security centers analyze information, often correlating information from numerous sources in an attempt to uncover threats along with their intensity [6]. Microsoft security scientists are continually vigilant for dangers. They approach a far-reaching set of telemetry picked up from Microsoft's worldwide nearness in the cloud and on-premises. This wide-coming to and different gathering of datasets empowers Microsoft to find new assault examples and patterns over its on-premises customer and endeavor items, just as its online administrations. Subsequently, the Security Center can quickly refresh its identification calculations as aggressors discharge new and progressively complex endeavors. This methodology encourages you to keep pace with a quick-moving risk condition [7].

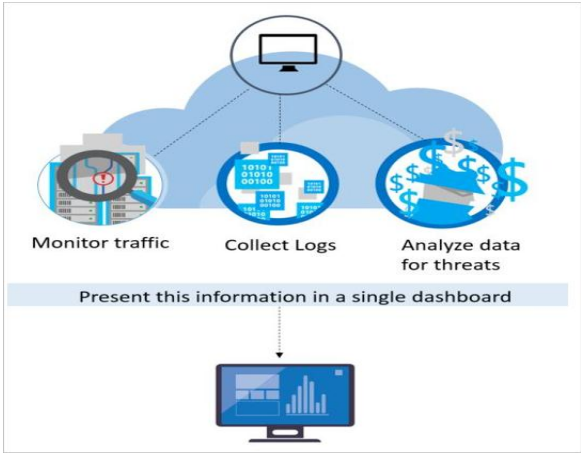

Figure 4: Security-center-detection-capabilities-fig1 [7]

Security Centre risk location works via consequently gathering security data from your Azure assets, the system, and associated accomplice arrangements. It dissects this data, frequently corresponding data from numerous sources, to recognize dangers. Security cautions are organized in Security Centre alongside proposals on the most proficient method to remediate the risk [7]. There some risk event type that is used to identify suspicious action or any risk event in Azure service. Some example of risk event type leaked or lost information, sign-ins from unknown IP addresses locations, doubtable locations, Sign-in from locations that are unidentified, Sign-ins from devices that may be infected, Sign-ins from IP addresses whose traffic is suspicious [8].

VI. SEVERITY RATE OF THE THREAT

Azure AD enables a user to control access to memberships, asset gatherings, and individual assets. This should be possible at the individual or gathering level, and by client job. The bigger the organization or, the more mind-boggling the framework, the more jobs you're probably going to have [9]. It's a good practice to encrypt your data while in transit and at rest [14].

Here are the lists of cloud security threats for that every organization might need to take prior actions. Cloud security threats as follows [10]. (a) Data breaches. (b) Abuse and nefarious use of cloud services. (c) System vulnerabilities. (d) Insufficient identity, credential, and access management are also kind of most significant thread for cloud service. (e) Malicious insiders. (f) Insufficient due diligence. (g) Denial of service. (h) Shared technology vulnerabilities. (i) Bonus cloud threat. (j) Account hijacking. (k) Advanced persistent threats. (l) Insecure interfaces for application programming interfaces.

VII. CONCLUSION

By following the agile Threat Modelling Express (TME) might be a solution to get maximum prevention from threats. Risk Modelling Express is a lightweight procedure to organize your application security endeavors. Given a four-hour meeting position, Threat Modelling Express (TME) fills the hole between a total nonappearance of plan security process and a far-reaching, formal methodology. TME assembles agreement from critical partners on dangers that issue to the business while catching both space freethinker and area clear dangers – the last which frequently requires personal investigation to find. We can consider cloud services. Cloud provides enough tools for secure development, operation and administration of system deployed on its platform [12].

REFERENCES

[1] C. Direct, "*An introduction to the Microsoft Azure portal*," Find your cloud solution, 2019. [Online]. Available: https://www.clouddirect.net/knowledge-base/KB0011450/an-introduction-to-the-microsoft-azure-portal. [Accessed: 28-Aug-2019].

[2] R. Riddle, "*7 Popular Azure Cloud Services for Enterprises*," Managed Dedicated, Cloud and Hosting Services, 27-Sep-2018. [Online]. Available: https://www.codero.com/resources/blog/7-popular-azure-cloud-services-enterprises/. [Accessed: 28-Aug-2019].

[3] L. Dignan, "*Top cloud providers 2018: How AWS, Microsoft, Google, IBM, Oracle, Alibaba stack up*," *ZDNet*, 12-Feb-2019. [Online]. Available: https://www.zdnet.com/article/top-cloud-providers-2018-how-aws-microsoft-google-ibm-oracle-alibaba-stack-up/. [Accessed: 28-Aug-2019].

[4] I. T. Connect, "*Azure AD Architecture*," IT Connect, 2019. [Online]. Available: https://itconnect.uw.edu/wares/msinf/design/arch/aad-arch/. [Accessed: 28-Aug-2019].

[5] R. L'Esteve, "*Azure Data Factory Mapping Data Flow for Datawarehouse ETL*," SQL Server Tips, Techniques and Articles, 17-Jun-2019. [Online]. Available: https://www.mssqltips.com/sqlservertip/6074/azure-data-factory-mapping-data-flow-for-datawarehouse-etl/. [Accessed: 28-Aug-2019].

[6] Monhaber, *"Security alerts in Azure Security Center*," Microsoft Docs, 2019. [Online]. Available: https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview. [Accessed: 28-Aug-2019].

[7] Monhaber, "*Security alerts in Azure Security Center*," Microsoft Docs, 2019. [Online]. Available: https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities#asc-detects. [Accessed: 28-Aug-2019].

[8] C. David. "*Introducing azure machine learning*." A guide for technical professionals, sponsored by Microsoft Corporation (2015).

[9] P. Joel, and V. A. Bharadi. "*Signature Verification SaaS Implementation on Microsoft Azure Cloud*." Procedia Computer Science 79 (2016): 410-418.

[10] B. Violino, "*12 top cloud security threats: The dirty dozen*," CSO Online, 11-Jun-2019. [Online]. Available: https://www.csoonline.com/article/3043030/the-dirty-dozen-12-top-cloud-security-threats.html. [Accessed: 28-Aug-2019].

[11] Sharif MHU, Datta R(2019). "*IDENTIFYING RISKS AND SECURITY MEASURES FOR E-COMMERCE ORGANIZATIONS"*. Retrieved from URL:

https://pdfs.semanticscholar.org/a2ec/8c072d9813d7e6e87c9ae01ec5a108f92467.pdf

[12] Sharif MHU, Datta R(2019). "*SOFTWARE AS A SERVICE HAS STRONG CLOUD SECURITY*". Retrieved from URL: https://www.researchgate.net/profile/Haris_Sharif/publication/335232826_Software_as_a_Service_has_Strong_Cloud_Security/lin ks/5d6466fc299bf1f70b0eb0f2/Software-as-a-Service-has-Strong-Cloud-Security.pdf

[13] Md Haris Uddin Shairf, Ripon Datta, Mounicasri Valavala (2019) "*Biometrics Authentication Analysis*". DOI : 10.14445/22315373/IJMTT-V65I10P506 Retrieved from URL: http://www.ijmttjournal.org/Volume-65/Issue-10/IJMTT-V65I10P506.pdf

[14] Sharif Md Haris Uddin, Ripon Datta(2019). "*Information Technology Security Analysis*". Retrieved from URL:https://www.researchgate.net/publication/336603051_Information_Technology_Security_Analysis

[15] A. Salma, C.Sarada Devi, V. Saranya, "*Smart Card for Banking with Highly Enhanced Security System",* SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – volume1 issue2, 2014.