11. About Problems and Requirements with Privileged Access and Authorization Management in Cloud-Based Multi-Tenant Networks

Marleen Steinhoff, Rakuten Mobile Inc., marleen.steinhoff@hm.edu
Sander de Kievit Rakuten Mobile Inc. sander.dekievit@rakuten.com

ABSTRACT

This paper gives an overview of the existing problems and requirements for privileged access to network functions in a virtual multi-tenant network. Cloud networks often use already existing solutions, and each solution is individually configured and build for different purposes. This leads to the following problems: First, using a variety of authentication methods leads to an inhomogeneous level of security for the different virtual functions in the network. Second, security policies differ from one solution provider to the other. Third, settings are set on different virtual functions locally and also on different layers of software which makes the authentication methods difficult to maintain. Simultaneously, by exploiting the authentication vulnerabilities, the possibility of attacks may increase. Thus, it is challenging, but crucial providing these network functions with secure access which includes strong authentication and holistic logging, in order to reduce the risk of incidents and detect attacks.

INTRODUCTION

Numerous companies in various sectors [1], [2], [3], [4] are transitioning to cloud-based solutions. The reason to do so is cost efficiency, scalability, and flexibility among others [5]. These cloudbased solutions, however, also need to be operated and maintained and therefore be accessible by system administrators. This paper underlines the challenges that emerge with access management in a cloud environment.

Cloud-based solutions can be separated into roughly two layers: the so-called “lower cloud” providing the hardware as well as the actual cloud infrastructure and the “upper cloud” which comprises of the network functions including software solutions from solution providers (SPs). The upper cloud also includes the application layer with the applications that can be actually used by an end-user. In this paper, we will use the words “in the cloud” to refer to the upper cloud and “cloud infrastructure” to refer to the lower cloud.

In order to build less expensive cloud-based networks quickly, using state-of-the-art solutions from other companies can be used. The resulting multi-tenancy is one of the main characteristics of cloud computing environments[1] [6].

Since solutions from different SPs provide and support many different authentication methods, authenticating users and giving them privileged access has become a complex issue. In addition, the users, like maintainers and developers, access the network from different entry points. The different channels used to connect to the functions in the network are complex to overview and to maintain. Furthermore, the 2019 Cloud Security Report analyzed that 31% of cybersecurity professionals have problems with setting consistent security policies in the cloud [7].

As the stability of the network depends on the availability of the functions within the network, the authorization of user actions after authenticating them is also an important factor. Users should not be able to perform critical actions to intentionally or unintentionally disable provided functions.

In case someone performed malicious actions, it’s essential to trace back those actions in order to restore the previous status, detect the entry point into the network and fix vulnerabilities. When different authentication

[1] defined by the National Institute of Standards and Technology

methods are used simultaneously, security measures such as logging can easily get bypassed, which leads to unauthorized access and incomplete or nonexistent logging.

Therefore, three main problems exist in cloudbased multi-tenant networks for privileged access management (PAM): An unpredictible amount of users from different environments access the network and need to get authenticated properly, the action has to be authorized for the requested resource, and actions on the virtual functions need to get logged securely without any exception for triggering alarms and for forensic purposes.

In this paper these problems are analyzed and the resulting requirements specified. Solutions for these problems have been developed already[2], but 72% of organizations still had public cloud related security incidents in the last year [7]. As a result, a more hollistic approach is needed to avoid incomplete security measures.

This paper is structured in the following way: Introduction, followed by the problems that occur in multi-tenant networks with regards to authentication and authorization, then resulting requirements are listed and finally it ends with the conclusion. The major problems are analysed in section II and the resulting neccessary requirements are explained in section III. Analysed problems are numbered (P + number) and the requirements refer to the problems they cover. Section IV summarises the main problems and requirements for a solution providing secure IDM (Identity Management) and PAM in a cloud network.

In this paper the following terms are used:

- multi-tenant networks: network build with seperate solutions, provided by different solution providers
- cloud provider: the owner of the cloud network
- cloud solution provider: builds, provides and maintains a software solution for the cloud network
- user: every subject or object connecting to a cloud solution from the tenant or cloud provider side, no end-users of the provided solution or network

PROBLEMS WITH ACCESSING CLOUD-BASED VIRTUAL FUNCTIONS

Most of the challenges cloud providers face about IDM and PAM are not neccessarily new in computer science, but the context has been drastically changed for cloud networks. This is due to heterogeneity in the provided solutions, the architecture of the virtual infrastructure itself, the distributed and decoupled character, and the increased amount of attack surfaces and complexity. Next to the well-known issues with IDM and PAM, cloud computing also comes with completely new categories of threats [11] challenging cloud and solution providers. The most relevant problems a cloud-based multi-tenant network comes with in terms of authentication and authorization are discussed in the following sections.

A. HETEROGENEITY IN CLOUD NETWORKS

Heterogeneity in cloud-based networks comes in different aspects: The variety of different solutions from different tenants used to build the cloud infrastructure, the different user groups accessing the network from various environments, and the different layers of infrastructure. These aspects create heterogeneity as well as complexity within the network. This heterogeneity further creates new problems regarding implementation and operation, making IAM (Identity and Access Management) one of the three main concerns existing for security improvement in cloud environments [12]. The problems that the different aspects of heterogeneity create are explained in the following subsections.

1) *Software Layers:* With cloud computing, new layers of software have been added to the infrastructure architecture. As every software layer needs to provide its own access methods for maintenance and change management on the layer itself, the provided remote access of the cloud layer increases the amount of possible vulnerabilities regarding access control and increases the complexity of the architecture in general. The increased complexity and additional authentication methods for the cloud layer increase the amount of potential

[2] Solutions for PAM in cloud environments such as from Entrust Datacard [8], BeyondTrust[9] or Saviynt[10]

vulnerabilities regarding authentication and authorization. Especially when access procedures are defined locally on the layer itself using weak authentication methods, these vulnerabilities can create a backdoor for attackers (P1).

Because efficient change management is a key factor in the success of a cloud environment [13], elements in a cloud network must be constantly changing, affecting every layer. Software is constantly changing as new features are added, faults are corrected, and code is restructured[14]. In the case of IDM and PAM, authentication protocols and cryptographic methods must also be supported to secure the authentication procedures. Therefore, authentication procedures not only have to be maintained, but also the changes have to be implemented (P2).

2) Variety of software solutions: Professor J. Joshi defined the heterogeneity of software solutions and hardware components as one aspect of heterogeneity in cloud environments [15]. As this paper focuses on authentication and authorization of users, hardware heterogeneity should not affect IDM and PAM procedures in cloud environments.

The heterogeneity of software solutions is created by the different solutions built for several purposes, e.g. business functions, management functions and security functions among others, built and provided from different SPs. The different needs require different authentication methods. One example is related to functions for logging purposes, these functions have to be tamper-safe and therefore require very strong authentication only for a very restricted selection of maintainers. A different authentication method is needed, when functions handle a large amount of users that stay logged in, e.g. for messaging software. Therefore, the virtual elements often have their own PAM solutions or interfaces implemented. The implementation is adapted to the functions' specific individual needs, including how often users access and use the service, how security-sensitive the software and stored data is and where the service is virtually and physically placed. In addition, different standards are used for authentication procedures depending on the individual needs and systems already in use (P3). The points mentioned above affect access management and security when the integrated solutions don't support the same access methods or when network settings, such as supported protocols or open ports, are set differently.

In case standards used in the network are not supported, the missing standards or interfaces have to be added and the settings have to be changed from every SP with hindsight. More likely, workarounds such as local authentication functions are implemented as the SPs already have invested significantly in their own authentication systems [12]. Also most services still rely on regular accounts [16], [17] stored locally on the cloud function itself making them susceptible to attacks (P4). This allows users as well as attackers to log into functions directly without using the official authentication methods. Consequently, workarounds and local logins can easily lead to incomplete logging when official authentication procedures are surrounded (P5). An incomplete logging makes it difficult or even impossible to trace back the path an attacker took within the network and what changes have been applied on the elements. For example, when the user logs in to a first function in the network using a central authentication procedure and then connects directly to another function using local credentials, the actions on the first functions will be logged properly, but the actions on the second function will most likely not be logged. A similar problem appears when the functions log executed actions, receiving the actual time from different systems (P6). Actions can't be traced back when the logs are generated using unsynchronized clocks.

Additionally, decentralized authentication also causes problems when changes on software are required. As the authentication software is installed on different functions, updating software and changing configurations takes a lot of effort and is extremely time-consuming. Furthermore, it's likely that changes are not holistically implemented which leads to vulnerabilities when some parts of the network still rely on previous versions (P7).

Even when a global authentication method is implemented for all functions in the network, a fall-back solution is needed when the main authentication method is out of service. These fall-back-solutions can act as backdoors for attackers when they enable an attacker to bypass the central authentication (P8). Especially when fall-back solutions are are defined locally, logging procedures can be completely circumvented (P9). In addition, locally defined or distributed user accounts are difficult to maintain, which can lead to unauthorized accounts existing on the elements and can create a backdoor for attackers (P10). As weak authentication methods act as an entry point into a network and compromise other functions, the easiest way into a network reduces the security level of the whole network.

The heterogeneity of software solutions in the network is not only chaotic, but also causes incompatibilities when using functions interconnected by coupling them. For IDM and PAM, these incompabilities come in two main aspects: Incompatible security policies and incompatible authentication methods. When different authentication methods are implemented and supported by the provided solutions, authenticating to a service and coupling it to another service can cause incompatibilities when the authentication methods from different SPs don't match [15] (P11). Consequently, either the elements trust already authenticated users once they are authenticated within the network, or the users have to get re-authenticated.

Incompatibility also appears in security policies, for example, when different password policies or protocols are allowed by different SPs. Different SPs define their own password policies, such as minimum required password length or allowed characters. The policies from different SPs vary and therefore don't provide the same level of security (P12).

Consequently, trust management between the implemented software solutions is fundamental for communicating policy together with validating and evaluating access credentials before trusting the other party [18]. This trust is essential not only between users and functions, but also between the functions themselves. If untrusted functions are allowed on the network and not validated, this can lead to vulnerabilities. Unknown functions can be placed in the network by an attacker when the authenticity is not validated (P13). Therefore, trust is one of the most concerned obstacles for the adoption and growth of cloud computing[19].

3) Different solution providers: When the network is not completely built by the cloud provider itself, solutions from other companies are used to build the network. This results in unclear roles and responsibilities in cloud networks [20] as responsibility is divided among different groups including the cloud user, the cloud tenant, and any third-party vendors [21].

While it is relatively clear who is responsible for the security of single provided functions, it is much more difficult to assign responsibilities for tasks that can influence the overall security of the network. The changes on authentication methods as they are needed to gain privileged access to every function in the network are an example. Even when the authentication method is considered as bug-free, it can cause vulnerabilities when the method is used in operation together with different elements in the network. As a result, it is unclear who takes responsibility of the overall security in the network (P14).

The same problem appears when changes have to be implemented, for example when providers want to apply software changes that affect the security of the cloud. The functions offered are provided by different companies as well as assigned to different teams within the company. The boundaries between responsibilities become blurred when it comes to the acutal assignment of tasks, for example, when the cloud provider chooses a framework, the solution is not configured for or when vulnerabilities need to get eliminated on the external provided software solution (P15).

Another problem that comes with the heterogeneity of solution providers is that the developers implementing the solutions are often not security experts, which leads to misconfigurations, buggy code and weak passwords exposing their services [22]. This is problematic when security-related functions as authentication or logging functions are implemented by developers without a review from security experts (P16).

4) Different user groups: Heterogeneity can also be found in the user groups since maintainers and developers of the cloud networks are coming from different companies with different backgrounds. As the users are connecting to virtual functions in the cloud remotely, authentication mechanisms are required to access the cloud through different entry points.

Even with properly maintained user accounts, the cloud provider does not know which persons or even objects use the privided accounts to access the cloud functions in the network. It is also not transparent to the cloud provider how SPs handle accounts, credentials and privileges on their side (P17).

As the users connecting to the cloud functions come from different environments, the amount of connecting users depends on the amount of solution providers as well as the number of people responsible for the project on the tenant's side. Therefore, the exact number of users is unpredictable in multi-tenant networks, which makes it challenging to avoid unauthorized users accessing the network or to avoid accounts of former users that are still accessible (P18).

B. CREDENTIAL MISUSE

For authentication of a user, it is checked whether a claimed identity corresponds to the actual identity on the basis of well-defined and unambiguous characteristics [23]. The characteristics in form of credentials are used to authenticate a user and therefore the key to remotely access every type of cloud network.

With regard to CSA's (Cloud Security Alliance) report "Top Threats to Cloud Computing - The Egregious 11", security incidents and data breaches can occur due to inadequate protection of credentials, failure to use multifactor authentication and failure to use strong passwords among others [24].

Using credentials that are easy to steal, guess or faked makes the access to a network vulnerable for attackers. In addition, authorized users from inside the network can misuse their access privileges. These attackers are known as malicious insiders. The problems behind both kinds of attacks, from inside and outside, are analysed in the following subsections.

1) External credential attacks: Almost every day, news about stolen user credentials, hacked databases and badly protected user accounts are reported. Also a report from (ISC)2[3] rated unauthorized access through misuse of employee credentials and improper access controls as the biggest perceived vulnerability to cloud security in their 2019 Cloud Security Report [7]. Once credentials are phished by attackers, it can lead to data breaches or misuse of access, financial damage through fines as well as a damage of reputation and customers trust.

The heterogeneity in the provided solutions as described in section II A 2), also affects the type of credentials used within the network. Even though the CSA and many other institutions [25], [26], [24], [20], [27] recommend the implementation of MFA (Multi-factor authentication) to protect sensitive data against unauthorized users, most organizations still heavily rely on passwords [17] (P19).

Passwords are easy to remember for users and simple to implement for SPs, but it leads users to reuse passwords accross different platforms and services or to write them down. Therefore, traditional authentication methods such as username and password are prone to password attacks and phishing and do not provide enough security in a cloud computing environment [25], [?]. Next to weak credentials, a lack of regular automated rotation of cryptographic keys, passwords and certificates leads to insufficient access management [24]

(P20). Once an attacker compromises credentials to an account, they can misuse the account as long as the credentials are valid. With credential rotation an attacker who already has access to the cloud network gets locked out.

But even when a secure authentication method is implemented troughout the whole network, an attacker can gain access to network functions using session hijacking. When the session is set up using URL rewriting or session tokens that get easily be stolen, an attacker can hijack the already existing session without having to authenticate (P21). In that case, a strong authentication method is being circumvented and doesn't offer secure access control against external attackers.

2) Malicious insiders: An insider is anyone in an organization with approved access, privilege or knowledge of information systems, information services, and missions [28]. Due to the previously mentioned multi-tenancy, many different groups of potential malicious insiders exist in cloud enviroments: cloud providers, solution providers and operations teams have access to the network and can misuse their access to the network. Malicious

[3] Non-profit-organization, Information System Security Certification Consortium

insiders aren’t a new issue, but the possible damage by malicious insiders is often far greater then in non-cloud-environments. This is due to the fact that cloud architectures necessitate certain roles which are extremely high-risk [20] regarding their privileges. The fact that malicious insiders already have privileged access to the cloud and their components puts them in a very powerful position. Therefore, 30% of cybersecurity experts see malicious insiders as the biggest security threat in public clouds [7].

In order to perform attacks, malicious insiders can use their privileges to gain access to internal resources and their insider knowledge to adversely impact an organization. Knowing about the system and authentication vulnerabilities and system configurations allows insiders to perform attacks easily. Bypassing authentication can easily lead to surrounding logging procedures or leaking information without being detected (P22). These opportunities make malicious insiders extremely theatening: ENISA (The European Union Agency for Cybersecurity) rated malicious insiders with a high risk to cloud environments [20], the Cloud Security Alliance[4] listed malicious insiders as one main threats in the “The Egregious 11” [24].

Since the behaviour of a malicious insider is distinct from external intruders, they cannot be detected using traditional intrusion detection methods [28] (P23). Also the additional software layer as described in section II A 3) gives malicious insiders even more enrty points to obtain access and perform attacks. As a result of their privileges and insider knowlege in combination with a different behaviour from outside attackers, the opportunities for temptations and influence are much higher, while it gets more difficult to detect them.

REQUIRED MEASURES FOR CLOUD-BASED ACCESS MANAGEMENT

The essential requirements arising from the problems explained in chapter II are defined in this section. Together they constitute a set of fundamental requirements for a secure access management solution with a hollistic apporoach. Requirements starting with ”I” are related to IDM,

”A” to PAM, ”S” to Session requirements, ”T” to Trust management, ”L” to Logging and ”C” to requirements regarding credentials and are written in italics. Problems defined in section II:

- P1: Authentication methods on different software layers creating backdoors for attackers.
    - *I5: A global access control policy for all elements shall be defined and accepted by all solution providers.*
    - *I4: Fine-granted access control systems shall be implemented.*
    - *I6: A security policy should be defined as the minimum required security level.*
    - *A5: A strong authentication method shall be implemented and reused within the network.*
    - *L1: Every security-related action shall be logged.*
    - *C2: The credentials shall have an expiration time.*
    - *C4: Credentials shall not be stored locally.*
    - *C5: Credentials shall be stored centralized, in a well-protected database.*
- P2: Authentication methods might have to be adjusted after changes in the environment
    - *A5: A strong authentication method shall be implemented and reused within the network.*
    - *A7: The central authentication method shall be easy to maintain and allows to apply changes easily.*
- P3: Different standards for authentication are used within the network
    - *I5: A global access control policy for all elements shall be defined and accepted by all solution providers.*
    - *T2: Secure authentication protocols should be defined for the whole network and no other protocols should be used.*
    - *A1: SSO should be implemented for functions from same network segment.*
    - *A3: Common account roles shall be defined for the whole network.*
- P4: Accounts and credentials are stored locally on the functions themselves

[4] the world’s leading organization dedicated to defining standards in cloud computing security

    - *I1: User accounts shall be stored centralized.*
    - *I2: User accounts shall be maintained.*
    - *I8: No local accounts shall exist on virtual elements.*
    - *C2: The credentials shall have an expiration time.*
    - *C4: Credentials shall not be stored locally.*
    - *C5: Credentials shall be stored centralized, in a well-protected database.*
- P5: Workarounds are existing, resulting into incomplete logging
    - A5: A strong authentication method shall be implemented and reused within the network.
    - L1: Every security-related action shall be logged.
    - L2: Logs shall be pushed to a well-protected logging backend.
    - C4: Credentials shall not be stored locally.
- P6: Functions receive the actual time from different systems
    - L6: Synchronized clocks shall be used across components.
- P7: Incomplete applied changes and updates within the network
    - I1: User accounts shall be stored centralized.
    - A5: A strong authentication method shall be implemented and reused within the network.
    - A7: The central authentication method shall be easy to maintain and allows to apply changes easily.
- P8: Weak protected fall-back solutions create entry point for attackers
    - I3: A well-protected fall-back solution should be implemented.
    - I4: Fine-granted access control systems shall be implemented.
    - I5: A global access control policy for all elements shall be defined and accepted by all solution providers.
    - I6: A security policy should be defined as the minimum required security level.
- P9: Incomplete logging due to locally implemented fall-back solutions
    - I3: A well-protected fall-back solution should be implemented.
    - I5: A global access control policy for all elements shall be defined and accepted by all solution providers.
    - I6: A security policy should be defined as the minimum required security level.
- P10: Unauthorized, distributed accounts exist on in the network
    - I1: User accounts shall be stored centralized.
    - I2: User accounts shall be maintained.
    - I8: No local accounts shall exist on virtual elements.
    - A6: The amount of root and admin accounts shall be reduced.
    - T3: Users connecting to virtual functions from other network segments shall be reauthenticated.
    - L1: Every security-related action shall be logged.
    - L2: Logs shall be pushed to a well-protected logging backend.
    - L3: Logs shall be held for a sufficient time, depending on the business case and regulations.
    - C2: The credentials shall have an expiration time.
- P11: Authentication methods from different solution providers are incompatible
    - I5: A global access control policy for all elements shall be defined and accepted by all solution providers.
    - I6: A security policy should be defined as the minimum required security level.
    - I7: Stronger authentication methods shall be implemented for security-sensitive functions.
    - T2: Secure authentication protocols should be defined for the whole network and no other protocols should be used.
    - A1: SSO should be implemented for functions from same network segment.
    - A5: A strong authentication method shall be implemented and reused within the network.
- P12: Security policies from different solution providers are incompatible

    - *I5: A global access control policy for all elements shall be defined and accepted by all solution providers.*
    - *I6: A security policy should be defined as the minimum required security level.*
- P13: Unknown functions can be placed in the network
    - *T1: The functions shall authenticate against other elements using certificates.*
    - *T4: Users shall only be accepted when they got authenticated from trusted instances.*
- P14: Unclear responsibilities for the overall security in the network
    - *I5: A global access control policy for all elements shall be defined and accepted by all solution providers.*
    - *I6: A security policy should be defined as the minimum required security level.*
    - *A5: A strong authentication method shall be implemented and reused within the network. The cloud provider is responsible for this central authentication method.*
- P15: Assignment of tasks is complicated when changes have to be implemented *see P14*
- P16: Missing reviews from security experts *A8: New software and changes on existing software of security-related functions shall be implemented from or reviewed by security experts.*
- P17: Unclear security standards including the handling of accounts and credentials *I5: A global access control policy for all elements shall be and accepted by all solution providers.*
    - I6: A security policy should be defined as the minimum required security level.
    - A9: The implementation and configuration of provided solutions shall be documented by solution providers.
    - C1: A MFA authentication should be implemented.
    - C2: The credentials shall have an expiration time.
    - C3: Keys and certificates shall have automatic credential rotation.
- P18: Accounts of former users are still accessible see P10
- P19: Passwords used for authentication without MFA
    - A5: A strong authentication method shall be implemented and reused within the network.
    - C1: A MFA authentication should be implemented.
- P20: Missing rotation of keys and certificates in the network
    - C3: Keys and certificates shall have automatic credential rotation.
- P21: The authentication procedure allows session hijacking
    - S1: Strong session management shall be implemented without weak tokens or URL rewriting.
    - S2: The session shall be disabled after the user logged out.
- P22: Malicious insiders can bypass authentication methods
    - I5: A global access control policy for all elements shall be defined.
    - I6: A security policy should be defined as the minimum required security level.
    - I8: No local accounts shall exist on virtual elements.
    - A5: A strong authentication method shall be implemented and reused within the network.
    - L1: Every security-related action shall be logged.
    - L2: Logs shall be pushed to a well-protected logging backend.
    - L3: Logs shall be held for a sufficient time, depending on the business case and regulations.
    - L4: Logging management solutions should be used.
    - L5: Notification and alerting rules shall be defined, the logging alone is not sufficient.
    - L7: An incident response and recovery plan shall be defined including clear responsibilities for operators.
    - L8: A security operations team should be build in order to identify and analyze security threats and react to them in a timely fashion.
- P23: Malicious insiders cannot be detected using traditional intrusion detection methods
    - A2: User role and used authentication method should be validated before giving access.
    - A4: The least privilege principle shall be applied.

- A5: A strong authentication method shall be implemented and reused within the network. I5: A global access control policy for all elements shall be defined.
- I8: No local accounts shall exist on virtual elements.
- L1: Every security-related action shall be logged.
- L2: Logs shall be pushed to a well-protected logging backend.
- L3: Logs shall be held for a sufficient time, depending on the business case and regulations.
- L4: Logging management solutions should be used.
- L5: Notification and alerting rules shall be defined, the logging alone is not sufficient.
- L7: An incident response and recovery plan shall be defined including clear responsibilities for operators.
- L8: A security operations team should be build in order to identify and analyze security threats and react to them in a timely fashion.

CONCLUSION

In conclusion, the existing problems regarding authentication and authorization in cloud environments can be categorized into four topics: Authentication methods and credentials, security policies, responsibilities and logging.

For authentication, locally implemented authentication methods and fall-back solutions can compromise the security of network functions themselves as well as other functions in the network. Especially then when weak credentials as passwords are used. Different authentication methods are often used within cloud-based networks which can cause incompatibilities.

The main problem for security policies is that every SP has defined their own policies and built solutions fitting their own requirements, leading to an unclear level of security for the whole network. Differing security policies also result into a lack of trust in the network between functions and authenticated users as well as among the functions themselves.

Assinging tasks becomes challenging when responsibilities are not clear. This affects the overall responsibility for security within the network as well as responsibilities for tasks that have to be assigned. Changes will always have to be implemented, otherwise workarounds are built in order to provide the missing functionality.

Allowing many channels to access elements including workarounds in the network can easily lead to an incomplete or insufficient logging as it becomes then possible to bypass the official logging procedures.

These problems require measures in order to secure and control access in the network. These measures shall cover a strong authentication method using MFA that is reused within the network. Fallback solutions, in case the central authentication method is out of service, shall be stored in a well-protected and centralized manner, therefore not locally. The same applies for locally stored credentials as it opens backdoors for attackers. For authentication between functions against each other, certificates shall be used to proof the identity and establish trust. For authenticating users within the same network segment, SSO (singlesign-on) solutions shall be used. A proper logging framework shall be implemented to log all actions that are security-related. This framework includes logging management and forensic solutions with clearly defined notification and alerting rules.

Additionally, security policies shall be defined. These are mandatory for all providers in order to be able to provide solutions for the network. Furthermore, the solution provider shall make a documentation of the implementations and configurations set on the provided function transparent to the cloud provider .

Currently, numerous solutions from different providers are offered for IDM and PAM, which often includes the individual implementation by the provider. However, these rarely cover all the individual needs of a heterogeneous cloud network. It is therefore necessary to work on a solution that is flexible enough to be adapted to the different needs, configurations and used standards without creating security gaps.

APPENDIX

This paper has been written as part of an internship at Rakuten Mobile as a student from the Munich University of Applied Sciences.

REFERENCES

[1] The top cloud providers for financial services.

[2] Rakuten is building the world’s first end-to-end cloud-native mobile network: Tareq amin.

[3] Volkswagen und microsoft treiben zusammenarbeit bei automotive cloud voran.

[4] Microsoft, bmw launch industrial cloud technology partnership.

[5] Mariana Carroll, Alta Van Der Merwe, and Paula Kotze. Secure cloud computing: Benefits, risks and controls. In *2011 Information Security for South Africa*, pages 1–9. IEEE, 2011.

[6] Timothy Grance Peter Mell. The nist definition of cloud computing.

[7] Holger Schulze. 2019 cloud security report.

[8] Cloud-based multi-factor authentication.

[9] Privileged remote access.

[10] Cloud privileged access management.

[11] John C. Grundy Amani S. Ibrahim, James H. Hamlyn-Harris. Emerging security challenges of cloud virtual infrastructure. *CoRR*, abs/1612.09059, 2016.

[12] P.G. Dorey and A. Leite. Cloud computing - a security problem or solution?

[13] Mukkamala R. Zubair M. Kaminsky D. AbdelSalam H., Maly K. Towards energy efficient change management in a cloud computing environment.

[14] Audris Mockus and Lawrence G Votta. Identifying reasons for software changes using historic databases. In *icsm*, pages 120–130, 2000.

[15] G.-J. Ahn H. Takabi, J.B.D. Joshi. Security and privacy challenges in cloud computing environments.

[16] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats Naslund, and Makan¨ Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, 1, 2016.

[17] The 3 biggest problems with password policies.

[18] I. Lee O. Sokolsky J. M. Smith A. D. Keromytis W. Lee M. Blaze, S. Kannan. Dynamic trust management.

[19] Talal H. Noor and Quan Z. Sheng. Trust as a service: A framework for trust management in cloud environments.

[20] Daniele Catteddu and Giles Hogben. Cloud computing benefits, risks and recommendations for information security. [21] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. *Communications of the ACM*, 53(4), 2010.

[21] Yogesh Mundada, Anirudh Ramachandran, and Nick Feamster. Silverline: Data and network isolation for cloud services. In *HotCloud*, 2011.

[22] Claudia Eckert. *IT-Sicherheit- Konzepte - Verfahren – Protokolle*.

[23] Jon-Michael C. Brook et al. Top threats to cloud computing: Egregious eleven.

[24] R. K. Banyal, P. Jain, and V. K. Jain. Multi-factor authentication framework for cloud computing. In *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, pages 105–110, 2013.

[25] Owasp top 10 - 2017.

[26] Michaela Iorga. Challenging security requirements for us government cloud computing adoption.

[27] Mark Maybury, Penny Chase, Brant Cheikes, Dick Brackney, Sara Matzner, Tom Hetherington, Brad Wood, Conner Sibley, Jack Marin, and Tom Longstaff. Analysis and detection of malicious insiders. Technical report, MITRE CORP BEDFORD MA, 2005.