Security Issues and Future Challenges of Cloud Service Authentication

Shu Yun Lim[1], M. L Mat Kiah[2], Tan Fong Ang[2]

[1]Faculty of Business Technology and Accounting, Unitar International University, 47301 Selangor Darul Ehsan, Malaysia; lim_sy@unitar.my

[2]Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia; misslaiha@um.edu.my, angtf@um.edu.my

Abstract: Authentication, in the cloud context, is the process of validating and guaranteeing the identity of cloud service subscribers or users. It is deemed essential since its strength directly impacts the reliability and security of the cloud computing environment. Many efforts, within in the literature, have surveyed cloud security and privacy, but lack a detailed analysis of authentication for the cloud. In view of the research gap and the importance of a valid authentication infrastructure, this survey critically investigates different authentication strategies and frameworks proposed for cloud services. This paper discusses the pros and cons of different authentication strategies and presents the taxonomy of the state-of-the-art cloud service authentication. The paper concludes with the open issues, main challenges and directions highlighted for future work in this relevant area.

Keywords: cloud computing; authentication; authentication-as-a-service; identity management; access control

1 Introduction

Cloud computing is widely adopted for delivering services such as data storage and management over the Internet. There are large varieties of cloud solutions and services to be accessed by a large number of devices such as workstations, smart phones and tablets. The security requirement becomes more complex with flexible content processing and sharing among a large number of users through cloud-based applications and services. When clouds contain applications from multiple organizations on a single managed infrastructure, application data is vulnerable not only to external attacks, but also to attacks from other organizations sharing the same infrastructure. Financial services corporations reported spending over a billion each year to safeguard against online security breaches. Unfortunately, these problems remained unsolved with many incidents of cloud service losing or corrupting user data. In the latest hit, Adobe suffered significant security breaches compromising the data of 2.9 million customers and valuable source code after the company shifts to a cloud-based delivery model [1].

The cloud environment being distributed, in nature, is facing challenges in managing user's identity, authenticating and authorizing users. Cloud service providers have access to the information stored by subscribers for authentication purpose and this presents a privacy issue to their private information. It is difficult for cloud subscribers or users to make sure the proper Service Level Agreement (SLA) rules are enforced since there is a lack of transparency in the cloud that allows the users to monitor their own information. Besides, cloud users who subscribed to multiple cloud services will have to store passwords in all the clouds for authentication and hence authentication data are replicated and withheld in multiple clouds. These redundant actions of exchanging authenticating data may lead to an exploit of the authentication mechanism.

From the cloud service providers' standpoint, managing and authenticating users in the cloud is becoming inevitably complicated. More specifically, the process of authentication, which is to verify an entity that is trying to access protected resources, is very visible to users. It directly influences their perception of trust. Cloud providers and brokers try to overcome security and privacy-related issues by offering security solutions to its customers. Security-as-a-Service (SEaaS) is a new instance of a cloud service model that delivers security solutions to enterprises by means of cloud-based services from the cloud. These services may be delivered in different forms, and Authentication-as-a-Service (AaaS) is one of the variants. AaaS is the new form of user authentication that cloud users should embrace for mitigating the risk of compromising sensitive information. However, when we look at authentication aspects of cloud computing, most discussions today point towards various forms of identity federation between clouds. As stated previously, there is no information in the literature discussing the authentication strategies and the architectural perspective of the components that together form a strong authentication system. This paper helps to bridge the gap in the literature that would be of interest to both academia and industry alike.

Section 2 provides the overview and the research approach undertaken to investigate cloud service authentication. The taxonomy of cloud service authentication security is presented in Section 3. Section 4 highlights the current state-of-the-art work proposed to authenticate cloud services and their potential problems. Finally, conclusions and directions for future research are identified in Section 5.

2 Overview

In this paper, we provide a survey of cloud service authentication strategies with the approach depicted in Figure 1. The NIST cloud security architecture [3] [4] is adopted and referenced for the baseline terms and definition. The taxonomy of cloud AaaS is proposed after deriving the main properties for cloud service authentication. Literature in the field is analyzed and the authentication strategies highlighted. The previous steps provide the input to derive the open issues and the future directions in the field of cloud service authentication.

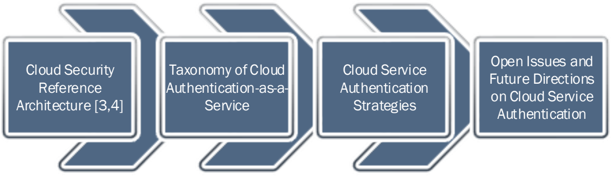

Cloud Security Reference Architecture [3,4]
Taxonomy of Cloud Authentication-as-a-Service
Cloud Service Authentication Strategies
Open Issues and Future Directions on Cloud Service Authentication

Figure 1
Research Methodology

Following the reference of NIST definition [3] and [4], the stakeholders involved in cloud service authentication are cloud providers, brokers, consumers, auditors and carriers. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from, a cloud provider. The cloud provider of SaaS assumes most of the responsibilities in managing and controlling the applications and the infrastructure, while the cloud consumers have limited administrative control of the applications. Cloud broker on the other hand is an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers. Different aspects of the secure cloud service management can be supported and implemented by either a cloud provider or by a cloud broker, depending upon the structure of each cloud ecosystem.

Meanwhile a cloud auditor is a party that conducts independent assessment of cloud services, information system operations, performance, and the security of a cloud computing implementation. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, and adherence to service level agreement parameters. A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. It provides access to consumers through network, telecommunications, and other access devices.

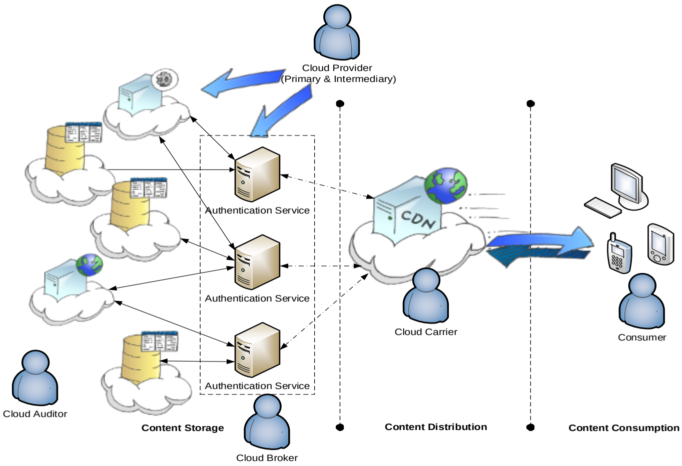


Figure 2
Stakeholders in cloud service authentication

3 Cloud Service Authentication Architecture

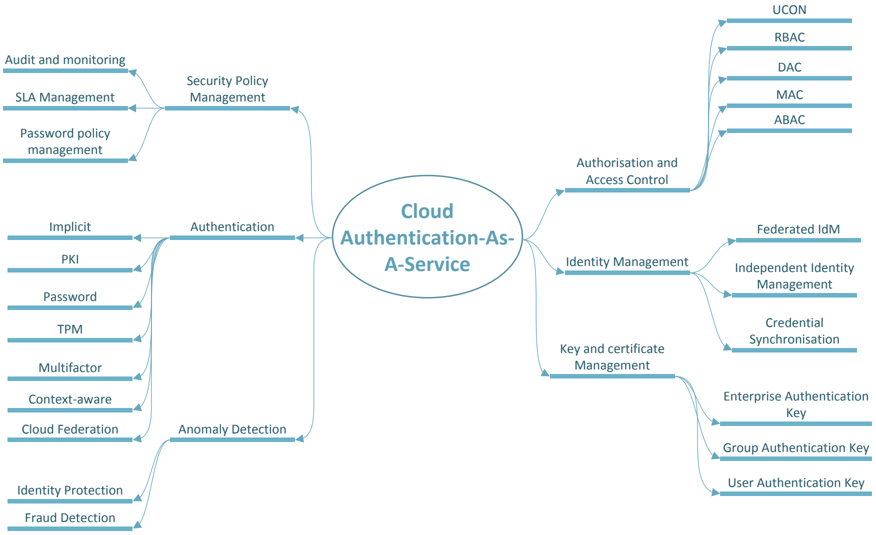


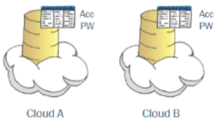
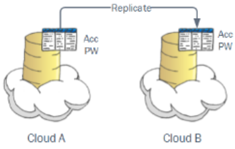
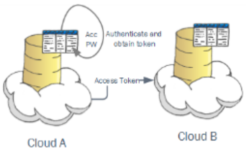
Figure 3
Taxonomy of cloud Authentication-as-a-Service

Both cloud providers and consumers are concerned about security issues associated with the cloud environment. Besides upholding the confidentiality of the system which is a generic security requirement across clouds, different cloud services may have different security and policy characteristics corresponding to specific functionality and usage of the system. The important aspects of cloud authentication service provisioning include Identity Management, Authentication, Access Control and Authorization, Security Policy Management, Key and Certificate Management and Fraud and Anomaly Detection. Taxonomy of the cloud service authentication infrastructure is presented in Figure 3.

3.1 Identity Management

Identity management (IdM) refers to the mechanisms and standards that create and maintain a cloud user's identity, and the de-provision of the user account when the user leaves the cloud service. IdM is a broad administrative area that deals with identifying individuals in a system and controlling access to the resources by placing restrictions on the established identities. Sound identity management and governance are needed to manage identities in hybrid cloud environments, a combination of cloud services and enterprise networks. Identity management in cloud involves three perspectives, namely the identity provisioning paradigm, the log-on paradigm, and the service paradigm [2]. Identity management is required to simplify the user provisioning process especially in enterprise environment. Enabling new users to get access to cloud services and de-provisioning users to ensure that only the rightful users have access to cloud services and data. This creation and deletion of identities are done without regard to user access rights to the service. The log-on paradigm involves exchanging of data by users to log-on to a cloud service. Lastly the service paradigm delivers personalized services to users and their devices after successful log-on attempts. There are three different models adopted by SaaS vendor to provide sign on and identity management service, namely independent IdM, credential synchronization, and federated IdM. Differences between the models are depicted in Table 1.

Table 1
Comparisons of IdM Model

IdM Model	Independent IdM	Credential Synchronization	Federated IdM
			 Acc PW Authenticate and obtain token Access Token Cloud A Cloud B
Description	• Consumer account information is managed by individual cloud	• Consumer account is replicated and information is shared between clouds	• Consumer account is managed independently

Strengths	• Easy to implement with no enterprise directory integration required	• Consumer manage fewer credentials	• No enterprise directory integration required • Lower risk as credentials are not replicated but propagated on demand
Weaknesses	• Consumers need to manage separate credentials for different accounts	• Requires integration with enterprise directory. • Higher security risk due to replication and distribution of consumer credentials	• Relatively more complex to implement • Require proper agreement and trust relationship between cloud services.

3.2 Authentication Strategy

Authentication is the process for confirming the identity of the user. Cloud consumers have to complete the user authentication process required by the cloud provider. The cloud provider can choose to provide different authentication mechanisms with different security strength and the strength depends on the reliability and integrity of the mechanism. Besides, authentication mechanisms must function properly in order to maintain data confidentiality and integrity. In view of the emergence of hybrid cloud environments, interoperability for user authentication has also become a major concern. The differences in authentication strategies are detailed in Table 2.

3.2.1 Password Authentication

Password authentication is simple and easy to use, but it has to have a certain level of complication and regular renewal to keep the security [3]. It is an authentication technology with well-known weaknesses in the sense that even if the correct username and password combination is provided; it is still difficult to prove that the request is from the rightful owner. Users frequently reuse their passwords when authenticating to various cloud services. Weak password practice brings high security risks to the user account information. Nonetheless, password authentication is still the most frequently used authentication technology with more than 90% of the transactions. Password authentication comes in different forms of challenge-response protocol in current cloud deployment.

3.2.2 Trusted Platform Module-based Authentication

Trusted Platform Module (TPM) is a hardware-based security module that uses secure cryptoprocessor that can store cryptographic keys that protect information. A variant of it, Mobile Trusted Module (MTM) [4] is a proposed standard by

Trusted Computing Group a consortium (TCG) founded by AMD, Hewlett-Packard, IBM, Intel, Microsoft. It is mainly applied to authenticate terminals from telecommunications. However, it is being considered as a cloud computing authentication method with Subscriber Identity Module (SIM) due to the generalization of smartphones. Cloud subscribers' devices can utilize unique hardcoded keys to perform software authentication, encryption, and decryption. TPM chips can also be used for other security technologies such as firewalls, antivirus software, and biometric verification. However, there are some inherent problems with the TPM technology, such as when an attacker manages to bypass disk encryption during a cold boot attack and reveal the master password with social engineering. In cloud environment, the biggest challenge is still the "Bring-your-own-device" (BYOD) concept that does not facilitate the implementation of TPM devices in enterprise network.

3.2.3 Public Key Infrastructure-based Authentication

Employing Trusted Third Party (TTP) services within the cloud leads to the establishment of the necessary trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and communication. The public key infrastructure (PKI), together with TTP, provide a technically sound and legally acceptable means to implement strong authentication and authorization. PKI is an authentication means using public-key cryptography. It enables users to authenticate the other party based on the certificate without shared secret information. One example of TTP authentication in cloud is Single-Sign-On (SSO). When a user gets authentication from a site, it can go through to other sites with assertion and no authentication process is required. However, the existence of a trusted third party, as an authentication server or certification authority, is becoming a security and fault intolerant bottleneck for systems.

3.2.4 Multifactor Authentication

Multi-factor authentication ensures that a user is who they claim to be by combining a few means of authentication. The more factors used to determine a person's identity, the greater the trust of authenticity [5]. ID, password, biometrics and certificates are used traditionally for single factor authentication. With the emergence of mobile network, second factor authentication takes the form of SMS, e-mail, and telephony OTPs, PUSH Notifications, and mobile OATH Tokens. Even though it is rather effective for closed communities such as enterprise cloud, these second factor methods are too costly, inconvenient, and logistically difficult especially for the distribution, administration, management and support in the cloud.

3.2.5 Implicit Authentication

This approach uses observations of user behavior for authentication and it is well-suited for mobile devices since they are capable of collecting a rich set of user information, such as location, motion, communication and their usage of applications. A number of profiling techniques have been studied to provide a suitable service for user and personal profile information in the mobile cloud environment [6] [7] [8]. But to date, a formal model for this approach has yet to be realized and limited device resources are the technical constraints that need to be overcome. Studies on intelligent mobile authentication service are still inadequate.

Table 2

Strengths and weaknesses of the authentication strategies

Authentication Strategy	**Strengths**	**Weaknesses**
Password Authentication	Simple to deploy	Regular renewal to keep the security due to deterministic function of storing password
Trusted Platform Module based authentication	Low deployment cost if TPM is integral part of an enterprise system Could be extended to incorporate other security services	Inherent TPM weaknesses such as cold-boot attack and master password revelation through social engineering BYOD does not facilitate TPM-based authentication in enterprise cloud
Public Key Infrastructure based authentication	Easy establishment of the necessary trust to provide cryptographically strong authentication solutions	Challenging certificate and key management in distributed environment
Multifactor authentication	Greater trust of authenticity	Logistically difficult for the distribution, administration, management and support in the cloud
Implicit authentication	Cloud subscriber device is capable of collecting a rich set of user information for profiling User authentication can be done dynamically, improves usability of authentication	Data collected for profiling risk disclosing user private information Limited device resources are the technical constraints to overcome
Context-aware cloud authentication	Context-aware cloud constantly retrieves structured information from users and profile users through active classification and inference User authentication can be done dynamically, improves the usability of authentication	Lack of privacy of user authentication data in the cloud

3.2.6 Context-Aware Cloud Authentication

While a full user and device profiling is not feasible as this stage, a context-aware cloud can assist in the dynamic and adaptive authentication method. Inherent components in this are enhanced authentication services, flexible access control and an adaptable security subsystem responding to current conditions in the environment. Since context-aware cloud constantly retrieves structured information from users and through active classification and inference, a model of the user who has legitimate access to systems and resources can be built. Given the characteristics of a context aware cloud, authentication can be done dynamically depending on the changing conditions of user's risk factor at a particular time. This type of risk-based authentication goes hand in hand with implicit authentication. It is a non-static authentication system which takes into account the profile of users requesting access to the system and relates the risk profile associated with that transaction. Higher risk profiles lead to stronger authentication need, whereas a static username and password may suffice for lower-risk profiles. Adapting authentication levels based on risk increases security beyond secret-knowledge techniques and provides transparent authentication without inconveniencing the user. Users continuously re-authenticate themselves to the cloud service to maintain confidence in their identity.

3.3 Authorization and Access Control

Authorization is of vital importance since it involves determining what the user is allowed to do after they have gained access. Authorization can be determined based on the user identity alone, but in most cases, it requires additional attributes about the user, such as their roles or titles. Meanwhile access control is more concerned with allowing a user to access a number of cloud resources. Though this process is typically handled by the applications being accessed, there is now consideration for centralizing the authorization policy decisions regardless of the location of the user or the application. The implementation of proper access control models for the cloud is one of the areas that has been critically evaluated since current access control models are not specifically designed to tackle the requirements of cloud systems.

As data and applications are shifted to the cloud, new challenges emerge to manage consistent and unified access policies for enterprises. Authorization is the means for ensuring that only properly authorized users are able to access resources within a system. An Authorization Service (AS) is responsible for evaluating an authorization query, collecting necessary information about the user and the resource, potentially from an attribute service and identity directory, and evaluating a policy to determine if access should be granted or denied.

Extensive research is being carried out in the area of access control in collaborative systems [9] [10], namely the Mandatory Access Control policies

(MAC), the Discretionary Access Control policies (DAC) and the Role Based Access Control policies (RBAC). Each one of them serves specific security requirements in different working environments. It is noteworthy that an attempt started along with the advancement of RBAC [11] for the design of a series of Attribute Based Access Control models (ABAC) [12] The ABAC model was mainly introduced to overcome a number of RBAC's shortcomings. Besides, UCON [13] [14] access control model is also introduced, along with RBAC, being the most prominent access control models for the Cloud. Nonetheless, further examination is demanded, due to the partial or weak fulfillment of security requirements in the Cloud.

3.4 Anomaly and Fraud Detection

The cloud consumer account and identity can be well protected by using a baseline user profile. Historical information about past user transactions, IP geolocation data, device authentication can be fed into a heuristic engine and by allowing the forming of user profiles, anomalies can be detected. Services such as fraud detection are also offered based on customized rules. Consumer transactions are analyzed in real-time to detect any activities that has similar patterns associated with crimes.

3.5 Security Policy Management

Security policy has become a critical concern of IT and businesses, in general. More specifically, security policy management in AaaS involves the SLA, password policy, audit and monitoring of the service. In order to properly audit the access or management of data governed by a cloud platform, all security operations based upon security identities and policies need precise audit information to be recorded. Meanwhile the purpose of the SLA is to define the basis for interoperable authentication or identity management solutions between consumers and providers [15].

3.6 Key and Certificate Management

Managing access to cloud services includes handling encryption keys and certificates. Key and certificate management have both been offered as part of the security to improve security, compliance and operational efficiency. In a case where the cloud service is being used to store a master encryption key, the data owner who deposited the key can define policies for how that key can be retrieved. This is important for establishing the necessary step in preventing unauthorized access and meeting compliance requirements for safeguarding keys. Centralizing management of keys and certificates on a cloud-based manager allows the storage of any security object, enforcement of retrieval and revocation policies, and prevention of unauthorized access to sensitive data and systems.

The implementation of key and certificate management service is not without its challenges. The additional complexity in cloud environments as compared to enterprise IT environments is due to the difference in ownership (between cloud consumers and providers) and the control of infrastructures on where the management system and security artifacts are located [16]. However with the correct implementation, this AaaS component provides an effective security layer against malicious attacks and streamlines the auditing process.

4 Related Work

In this section, solutions that have been proposed in academic research pertaining to cloud service authentication is presented and discussed. A summary of the literature presented in Table 3. Authentication architecture and approaches are illustrated in Figure 4.

4.1 Trusted Platform Module-based Authentication

A. Ahmad et al. proposed that cloud services rely on the existing International Mobile Subscriber Identity (IMSI) and Universal Subscriber Identity Module (USIM) cards for authentication [17]. Since mobile network authentication in GSM/ 3G/ WLAN is the first level of security authentication for a mobile subscriber, it could be a valuable asset for the security foundation of cloud computing. The framework includes a mapping between users and services, to determine if a user may access a specific service; and a mapping of IMSIs and user IDs to be recognized as the same user, allowing multiple devices to share the same account. By expanding the use of the trusted platform and USIM, and the introduction of virtualization, mobile cloud services authentication can be achieved.

Z. Song et al. proposed TrustCube [18], a policy-based cloud authentication platform using open standards that supports the integration of various authentication methods. The scheme uses Trusted Computing technologies like TPM, TNC and remote attestation to ensure trust in users, platforms and environment of the platform. The scheme includes an Integrated Authenticated (IA) Service that retrieves policy for access request, extract information and send inquiry to IA server though a trusted network. TrustCube is an end-to-end infrastructure that offers measurements of essential elements of clients, platform and the environment. The cloud service can make an informed decision based on the certifiable report of measurements. Besides, cloud service can also evaluate the risk of dealing with particular users. The authentication phase is token-based, where successful authentication a token is generated and used for further request from the same user. Biometric characteristics such as fingerprints and palm veins are used to provide biometric reference data in a shared secret key calculation. Nonetheless the proposal is based on the Trusted Platform Module (TPM) of corresponding clients' device for generating secure keys and detecting changes to client's platform (Figure 4, authentication flow 3). However, this is not feasible when enterprise users bring their personal smartphones and tablets into the workplace and use them to access corporate networks. The idea of BYOD (Bring Your Own Device) presents a unique security challenge for IT organizations and is driving the need for stronger authentication and access control policies on employee-owned mobile devices.

4.2 Implicit Authentication

R. Chow et al. proposed a flexible platform [8] for supporting authentication decision based on a behavioral authentication approach [6] [19], to translate user behavior into authentication score and thus allowing users to access cloud services transparently (Figure 4, authentication flow 3). This approach results in a new authentication paradigm which successfully strikes a balance between usability and trust. However, these behavior profiling techniques proposed have not been successfully implemented for mobile computing platforms due to complexity and intensive computation.

4.3 Context-Aware Cloud Authentication

Covington, M. J., *et al.* [8] proposed that context aware cloud to focus on security services incorporating the security-relevant context, making policy enforcement and access control flexible within a system-level service architecture. Manjea Kim et al. [20] and H. Jeong *et al.* [7] on the other hand make use of the context-aware platform of the cloud and proposed a scheme that considers user's context information and profile for authentication (Figure 4, authentication flow 1&2). This platform is able to gather the users' personal information and preferences as well to provide suitable services for them. The scheme includes methods that interpret and infer the high level context and resources management technique that manages distributed IT resources effectively. Further to that, H. Ahn *et al.* extended the context aware cloud authentication to include access control [21] [22]. The authors proposed a context-aware RBAC model which provides efficient access control to user through active classification, inference and judgment of the users assessing systems and resources.

4.4 Public Key Infrastructure-based Authentication

Many efforts have been made to improve identity management and authentication for cloud computing. Most of them focus on designing a trusted third party (Figure 4, authentication flow 2). For instance, Z. Wang *et al.* [23] [24] constructed a TTP with a homomorphic signature for identity management and access control in mobile cloud computing. In the identity management scheme, a mobile user firstly computes a full signature on all his sensitive personal information and stores it in a TTP. During the valid period of the full signature, the user can authenticate his/her identity to the cloud service provider through TTP. Meanwhile, for authorization and access control, a user's full signature on all identity attributes is stored in advance in the access controlling server. For a user who wants to access a cloud service, which has special requirement on one's identity attribute, the user only needs to notify the access controlling server of the particular cloud service name. According to the user's instruction, the access controlling server can compute a partial signature on the special identity attribute, and send it to the cloud server for identification. However, the scalability and extensibility of this scheme are under scrutiny. In the event of identity addition, update and removal, a full signature computation is required. This is very time-consuming and costly due to the heavy computation, and users are usually on very limited computational resources.

H. Li *et al.* [25] and Qin B. *et al.* [26] both proposed a framework for secure authentication and data upload in an identity-based setting. The identity-based feature eliminates the complicated certificates management in signature encryption schemes in the traditional public key infrastructure (PKI) setting. Besides, Mishra, D. *et al.* proposed another identity-based mutual authentication in cloud storage sharing using Elliptic Curve Cryptography (ECC) and claimed that their scheme can resist various attacks in the cloud infrastructure [27].

4.5 Password Authentication

Password-based authentication is relatively easy to construct and deploy (Figure 4, authentication flow 1). However in cloud deployment, without the randomization of password, a user is susceptible to dictionary attacks since the server has a deterministic function of the user's password. To overcome such a limitation, the authentication protocol must be a challenge-response type protocol where the server never learns any deterministic function of the client's password. Besides, to prevent malicious servers and cross-site impersonation, we require that the server never learn the client's password. Asymmetric Password-Authenticated Key Exchange (APAKE) attempts to remedy this problem. Only the client knows the password, while the server stores a one-way function of the password. However, APAKE schemes are still vulnerable to dictionary attacks to the server. Other notable research in this area includes single-password authentication scheme [28] and a multi-level authentication technique which generates and authenticates the password in multiple levels to access the cloud services [29]. A more secure scheme is the multi-factor authentication that requires a second factor (such as finger print, token, OTP) with username/password proposed by [30] [31]. Nevertheless, the feasibility of two-factor authentication is largely limited by high device cost and the deployment complexity.

4.6 Cloud Federation Authentication

Federated identity is a useful feature for identity management and single sign on. OAuth, OpenID and SAML are the main concepts for federated cloud service authentication (Figure 4, authentication flow 2). Celesti A. *et al.* [32] proposed the "Horizontal Federation" of cloud resources. One cloud service provider, lacking in internal resources, can cooperate with another cloud service provider in order to supplement required resources by means of external ones. The model consists of three phases: discovery of available external cloud resources, matchmaking selection between discovered cloud providers, and authentication for trust context establishment with selected clouds. The main focus of this model is the authentication phase, which is the cloud SSO. Through Cloud SSO a cloud provider authenticates itself with other heterogeneous cloud providers regardless of their implemented security mechanism and accesses all needed external cloud resources. In order to establish trust relationship between home and foreign clouds, a trusted Identity Provider is required to verify digital identities of clouds and provides SAML authentication assertions.

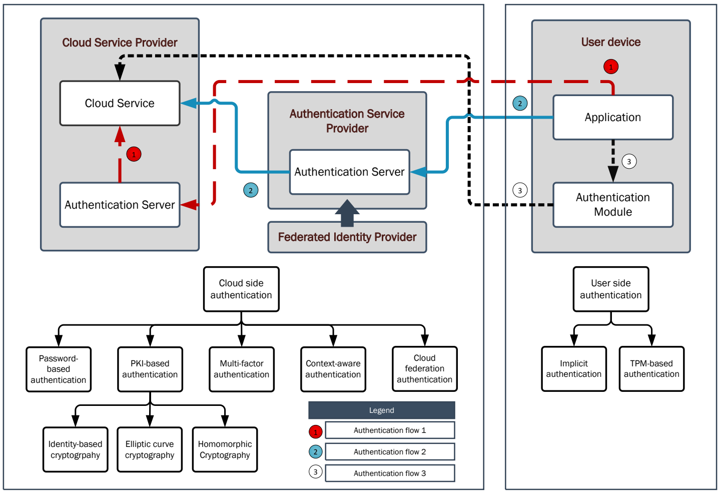


Figure 4
Authentication architecture and strategies

Table 3
Summary of the evaluated cloud service authentication schemes

Scheme	**Basic Theory**	**Type**	**Description**	**Idm**[1]	**Auc**[2]	**Ac**[3]
[20]	Context aware profiling	User profiling	Context aware architecture with user profiling	No	Yes	Yes
[7]	User profiling	User profiling	User profiling for mobile cloud authentication	No	Yes	Yes
[21]	Context aware profiling	User profiling	Context aware architecture with user profiling and RBAC for access control	No	Yes	Yes
[33]	Group Location-based security framework	TPM, Risk-based	Authentication with IMSI and location based service	No	Yes	No
[23]	Homomorphic Signature	PKI,TTP	Access control using Boneh-Boyen signature	No	Yes	Yes
[24]	Homomorphic Signature	PKI,TTP	Homomorphic signature for identity management and access control	Yes	Yes	Yes
[25]	Identity-based cryptography	PKI,TTP	Identity-based authentication protocol for cloud services	No	Yes	No
[30]	Anonymous One-Time Password	Password, PKI	Two factor authentication with OTP & RSA signature	No	Yes	No
[27]	Identity-based cryptography	PKI,TTP	Identity-based (ECC) authentication framework	No	Yes	No
[29]	Password concatenation	Password	Multi-level password concatenation for authentication	No	Yes	No

[1] Identity Management

[2] Authentication

[3] Access Control

[8]	User profiling	Implicit, Risk-based	Cloud authentication framework with behavioral authentication approach	No	Yes	No
[6]						
[28]	Single password authentication	Password	Challenge-response authentication protocol for cloud	No	Yes	No
[32]	Cross cloud federation authentication	Cloud federation	Cloud federation authentication	Yes	Yes	No
[34]	Cross cloud federation authentication	Cloud federation	Cloud federation authentication in enterprise	Yes	Yes	Yes
[17]	Trusted Platform Module based authentication	TPM, TTP	USIM/SIM-based authentication framework	No	Yes	No
[18]	Trusted Platform Module based authentication	TPM, biometrics	End-to-end Infrastructure built on TPM for authentication	No	Yes	No

5 Open Issues and Future Directions

Based on the related literature, there are several issues that have not been sufficiently addressed. The gap in the existing solutions would prove to be the direction for future work.

5.1 Privacy of Authentication Data

Although an issue of paramount importance, little research has been carried out in this regard. Existing cryptographic techniques can be utilized for data security but privacy protection and outsourced computation need significant attention. Personal data should always remain in the user control, and the user decides what and whom they share their data with. Especially when implicit and context aware cloud authentication strategy is used, the identity provider needs access to real-time information about the user. They need to feel confident when supplying their context information for profiling and authentication, and at the same time ensure that their privacy would not be violated.

Furthermore, data in the cloud typically resides in a shared environment. Even with SLA in place to support contract negotiation and enforcement, privacy and trust are non-quantitative and thus difficult to bargain. The challenge is that only authorized entities can access the data. There is a need for appropriate mechanisms to prevent cloud service providers from misusing customer's data.

5.2 BYOD Challenge in the Cloud (Bring Your Own Device)

Along with the growth of mobile consumer devices in the enterprise cloud, securing various types of employee-owned device access to cloud services has become a critical component of the IT value-chain. Unfortunately, classical authentication mechanisms, such as TPM-based authentication cannot respond to the new challenges. BYOD also brings true challenge to develop access control policies in enterprise and hybrid cloud environment.

5.3 Usable and Scalable Authentication

Research should be focusing on the ability to deliver authentication services that are considered usable and scalable across cloud environments. They also should be easy to learn, use, administer, and inexpensive to maintain. The question remains in how the usability of authentication mechanism can be improved, where user logs in once and gain access to all services without being prompted to log in again at different cloud service. Identity federation is the way to go but solutions and control policies must be enforceable across clouds which are difficult to coordinate. While implicit and adaptive type of authentication is trying to increase the usability of the authentication by making authentication as transparent and seamless as possible, they have yet to provide sufficient confidence in realizing a full secure authentication mechanism.

5.4 Future Work

Future research can be directed at putting trust back to the users to ensure that they are in full control of their data. In order to instill the trust in cloud users, cloud provider's technical competency has to be enhanced and at the same time the data owner should have full control over who has the right to use their data and what they are allowed to do with it once they gain access. This is where homomorphic encryption comes into the picture. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a desirable feature in modern communication system architectures that allow us to maintain confidentiality and privacy of outsourced data in cloud. With homomorphic encryption, only the users are equipped with encryption keys while operations are allowed over encrypted bits. This advancement put the trust back to the users that they are in full control of their data.

In addition to the increasing dominance of the mobile device as a primary point of access to cloud services, Cloud Security Alliance (CSA) specifically highlighted the need to provide usable and scalable authentication from mobile devices to multiple, heterogeneous cloud providers as an important step toward the maturity of cloud solutions. Current cloud-based authentication service offers solutions like single sign-on (SSO) to help simplify the management of access to services both in the cloud and behind the firewall. Single Sign-On has inherited the limitation of a password-based authentication and poses significant risks. Besides, its usability has rarely been investigated. In SSO once a user entered its credentials, the user gets signed in to all the subscribed services and re-authentication is required only after the credential is stale or time-out. This undeniably exposes users to more threats and security attacks. We suggest re-authentication when user is requesting for different types of service with different security requirements. In this case users re-enter credential only when the need arises and this can be a risk-based decision. With user risk profiling in place, an authentication service can then decide if the requested service implicitly needs a fresh authentication based on the risk factor. A risk profile of the cloud user is to provide a non-subjective understanding of risk by assigning numerical values to variables representing the threats and danger the user pose. It can be a useful tool for determining the magnitude of authentication required in cloud service authentication. Authentication that requires user mediation only when necessary addressed both the security and usability challenges.

Conclusion

Significant opportunities exist today to develop a strong cloud service authentication mechanism. A complete solution that incorporates identity management, authentication mechanisms, authorization and access control will make a substantial contribution to a correct and effective system of authentication. Organizations must ensure that service providers provide the flexibility to deliver varying levels of strong authentication to meet the required security policies and extend existing security implementations by incorporating identity federation. Addressing the security and usability challenges is a good direction in which to go and a more promising open standard authentication mechanism is needed to achieve a secure cloud ecosystem.

References

[1] Brandon, J., Adobe data breach highlights the company's security shortcomings, experts say. 2013

[2] Subashini, S. and V. Kavitha, A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011. 34(1): pp. 1-11

[3] Keszthelyi, A., About Passwords. Acta Polytechnica Hungarica, 2013. Vol. 10, No. 6

[4] Recordon, D. and B. Fitzpatrick, OpenID Authentication 1.1. Finalized OpenID Specification, May, 2006

[5] Nagaraju, S. and L. Parthiban, SecAuthn: Provably Secure Multi-Factor Authentication for the Cloud Computing Systems. Indian Journal of Science and Technology, 2016. 9(9)

[6] Markus Jakobsson, E.S., Philippe Golle, Richard Chow, Implicit authentication for mobile devices, Proceedings of the 4th USENIX conference on Hot topics in security. 2009, USENIX Association: Canada. p. 9-9

[7] Jeong, H. and E. Choi, User Authentication using Profiling in Mobile Cloud Computing. Aasri Conference on Power and Energy Systems, 2012. 2: pp. 262-267

[8] Chow, R., et al., Authentication in the clouds: a framework and its application to mobile users, Proceedings of the 2010 ACM workshop on Cloud computing security workshop. 2010, ACM: USA. pp. 1-6

[9] De Capitani di Vimercati, S. and P. Samarati, Mandatory Access Control Policy (MAC), in Encyclopedia of Cryptography and Security, H.A. van Tilborg and S. Jajodia, Editors. 2011, Springer US. pp. 758-758

[10] Sandhu, R.S. and P. Samarati, Access control: principle and practice. Communications Magazine, IEEE, 1994. 32(9): pp. 40-48

[11] Tang, Z., et al., A new RBAC based access control model for cloud computing, in Advances in Grid and Pervasive Computing. 2012, Springer. pp. 279-288

[12] Ruj, S., M. Stojmenovic, and A. Nayak, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds. Parallel and Distributed Systems, IEEE Transactions on, 2014. 25(2): pp. 384-394

[13] Park, J. and R. Sandhu, The UCON ABC usage control model. ACM Transactions on Information and System Security (TISSEC), 2004. 7(1): pp. 128-174

[14] Danwei, C., H. Xiuli, and R. Xunyi, Access Control of Cloud Service Based on UCON, Cloud Computing, 2009, Springer Berlin Heidelberg. pp. 559-564

[15] Brussels, Cloud Service Level Agreement Standardisation Guidelines. 2014

[16] Chandramouli, R., M. Iorga, and S. Chokhani, Cryptographic Key Management Issues and Challenges in Cloud Services. 2014: Springer

[17] Ahmad, Z., et al., Considerations for mobile authentication in the Cloud. Information Security Technical Report, 2011. 16(3-4): pp. 123-130

[18] Song, Z., et al., TrustCube: An Infrastructure that Builds Trust in Client, in Future of Trust in Computing, 2009, Vieweg+Teubner. pp. 68-79

[19] Hocking, C.G., et al., Co-operative user identity verification using an Authentication Aura. Computers & Security, 2013. 39, Part B: pp. 486-502

[20] Manjea Kim, H.J., Euiin Choi, Context-aware Platform for User Authentication in Cloud Database Computing. 2012

[21] Ahn, H., et al., User Authentication Platform Using Provisioning in Cloud Computing Environment, in Advanced Communication and Networking, 2011, Springer Berlin Heidelberg. pp. 132-138

[22] Ahn, H., et al., User Authentication Using Context-Awareness RBAC Model on Cloud Computing, in Future Communication, Computing, Control and Management, 2012, Springer Berlin Heidelberg. pp. 253-257

[23] Wang, Z., K. Sha, and W. Lv, Slight Homomorphic Signature for Access Controlling in Cloud Computing. Wireless Personal Communications, 2013. 73(1): pp. 51-61

[24] Wang, Z., G. Sun, and D. Chen, A new definition of homomorphic signature for identity management in mobile cloud computing. Journal of Computer and System Sciences, 2014. 80(3): pp. 546-553

[25] Li, H., et al., Identity-Based Authentication for Cloud Computing, in Proceedings of the 1st International Conference on Cloud Computing. 2009, Springer-Verlag: Beijing, China. pp. 157-166

[26] Qin, B., et al., Simultaneous authentication and secrecy in identity-based data upload to cloud. Cluster Computing, 2013. 16(4): pp. 845-859

[27] Mishra, D., V. Kumar, and S. Mukhopadhyay, A Pairing-Free Identity Based Authentication Framework for Cloud Computing, in Network and System Security, 2013, Springer Berlin Heidelberg. pp. 721-727

[28] Acar, T., M. Belenkiy, and A. Küpçü, Single password authentication. Computer Networks, 2013. 57(13): pp. 2597-2614

[29] Dinesha, H.A. and V.K. Agrawal. Multi-level authentication technique for accessing cloud services. International Conference on Computing, Communication and Applications (ICCCA), 2012

[30] Yassin, A., et al., Cloud Authentication Based on Anonymous One-Time Password, in Ubiquitous Information Technologies and Applications, 2013, Springer Netherlands. pp. 423-431

[31] Abdellaoui, A., Y.I. Khamlichi, and H. Chaoui, A Novel Strong Password Generator for Improving Cloud Authentication. Procedia Computer Science, 2016. 85: pp. 293-300

[32] Celesti, A., et al. Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication. in Advances in Future Internet (AFIN), 2010 Second International Conference on. 2010

[33] Chen, Y.-J. and L.-C. Wang, A Security Framework of Group Location-Based Mobile Applications in Cloud Computing. 2011: pp. 184-190

[34] Noureddine, M. and R. Bashroush, An authentication model towards cloud federation in the enterprise. Journal of Systems and Software, 2013. 86(9): pp. 2269-2275