Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 87-94 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

OVERALL REVIEW OF THE AUTHENTICATION PROBLEM IN THE CLOUD SERVICES

Oksiiuk O[1]., Vialkova V[2]. Chaikovska V[3]., Shestak Y.[4]
1-4 Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ABSTRACT. This article presents the secure authentication in cloud technologies and determining vulnerabilities in the algorithms. The research performs the development direction of the authentication protocols and their analysis. It is needed to identify the legislation and standards in the research field. After that, the threats investigation is the most crucial part, as we need to protect all vulnerable elements in the authentication process. The importance of such research is the rapid growth of the cloud technology industry. The result is offering new methods in the authentication algorithms.

Keywords: authentication, protocols, confidential information, secure connection, information security, cloud services, cybersecurity, threats, data storage, legislation, authentication algorithms, data protection.

1. Introduction

The term cloud services is a full category that encompasses the myriad IT cloud-based resources provided over the internet. Cloud-based means giving different services over the internet and all you need for accessing them is a connection to the internet and device that can do it.

The usage of cloud services has become associated with everyday cloud products, such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Examples of cloud services include online data storage (like google drive) and backup solutions, Web-based e-mail services (like Outlook Mail on the Web), database processing (like some tools in SPSS), managed technical support services and more.

As you can see, there are a lot of tools that cloud services can offer. That is why more companies and people at all decide to use them. The most challenging question here is protection the authentication process. The pieces of evidence of this are the papers written by different scientists around the globe like Deepanshu Goyal, M. Bala Krishna “Secure framework for data access using Location-based service in Mobile Cloud Computing”, J. Angela Jennifa Sujana, T. Revathi “Ensuring Privacy in Data Storage as a Service for Educational Institution in Cloud Computing”; Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar “Efficient Cloud Computing with Secure Data Storage using AES”; Dimitrios Zissis, Dimitrios Lekkas “Addressing cloud computing security issues”; H A Dinesha, V K Agrawal “Multi-level authentication technique for accessing cloud services”; Slawomir Grzonkowski, Peter M. Corcoran, Thomas Coughlin “Security analysis of authentication protocols for next-generation mobile and CE cloud services Sign In or Purchase” and more.

The authentication into the cloud services has the following features:

- Every company will have its identity management system to control access to information and cloud services. Cloud providers either integrate the customer’s identity management system into their infrastructure, using federation or SSO technology or a biometric-based identification system or provide an identity management system of their own.
- CloudID provides privacy maintaining cloud-based biometric validation. It leads the users' confidential information to their biometrics and stores it in an encrypted appearance. Making use of a searchable encryption technique, biometric identification is performed in the encrypted domain to ensure that the cloud provider or attackers do not get access to any sensitive data.

- Data confidentiality is the attribute that data contents are not accessible or disclosed to unauthorized users. Outsourced information is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information about the data. Meanwhile, data owners expect to utilize cloud data services fully.
- Access controllability means that a data owner can perform the selective restriction of access to his data outsourced to the cloud. Authorized users can be authorized by the owner to access the data and others cannot reach it without permission. Only the owner in untrusted cloud environments must control the access authorization.
- Data integrity demands to maintain and assure the accuracy and fullness of data. A data owner expects that their data stored in the clouds has to be stored correctly and reliably. It means that the data must not illegally interfere, somehow modified, consciously deleted, or maliciously faked. If any undesirable operations damage or remove the data, the user should be able to identify if something went wrong.

The resulting methods allow minimizing the risks in the authentication process. It shows that topic of research devoted to the vulnerabilities in the authentication algorithms to the cloud services is urgent.

The results reveal the importance of the law background in the information security at the national level. It has demonstrated the need for secure connection to add more methods of the authentication. In addition, users have to use the most convenient tool for the accessing on their devices.

2. Formulation of the problem

This paper presents the secure authentication in cloud technologies and determining the vulnerabilities in the algorithms. The research performs the development direction of the authentication protocols and their analysis.

The object of the study is the threats of the authentication in cloud technologies. The subject of research is vulnerabilities in the authentication algorithm. The analysis based on the comparison of the protocol, synthesis of the main features and reviewing the results.

It was determined the following tasks for achieving the goal:

- Analysis of the legislation in cloud services security.
- Identifying the threats of the authentication process to the clouds.
- Study of the vulnerabilities in the current authentication protocols.

3. Data protection law in the cloud services

It is essential to find a way to settle all aspects of the dispute that can be everywhere. We cannot avoid this regulation in the cloud technologies, as a lot of people decide to use this storage method instead of hard drives.

We can find in Ukrainian law only general thesis that international society requires. Here it is the law about information (02.10.1992), about the State Service for Special Communications and Information Protection of Ukraine (23.02.2006), about information protection in the information and telecommunication systems, about government secrets, etc. If we analyze all these documents, we can find only general terms that can protect nobody. Such tendency creates an excellent place for cybercrimes.

However, such situation has a place not only in Ukraine, but it also has a place in more countries that it should be.

Much can be learned from countries that have been able to reduce threats in clouds. Such states are the UK, US, Germany, and Japan.

The legislation creates a legal a basic structure underlying a concept to resolve the progressively frequent severe disagreements between the United States and foreign countries over access to outside data stored. The fundamental legitimate question is that of external jurisdiction which the legal system of one country can extend to another country. Examples of such areas include terrorism and piracy.

Policy in this area tends to focus on moving government agencies to cloud services. One example is the Cloud First Initiative, launched by former US government CIO Vivek Kundra, which aimed to cut waste and increase efficiencies within the US federal government's technology services by reducing government IT expenditures by US$4 billion dollars over the next two years. As one result of this initiative, the General Services Administration, the federal government's procurement agency, has developed some resources to assist government agencies in procuring cloud services. More recently, President Trump recently signed an Executive Order on cybersecurity mandating that federal systems move to the cloud.

The act amended US law to make clear that law enforcement warrants can apply to data that the United States based technology corporations have stored anywhere in the world. It also gives those enterprises the right to challenge these licenses based on the privacy laws where the data are stored.

British data protection laws make the UK one of the best places in the world to adopt cloud computing services, according to new research. The yearly ranking is designed to help countries find an equivalent for their current policies and identify the following levels for increasing adoption of cloud computing. Researchers referenced Ministers' decision to incorporate the EU's General Data Protection Regulation into UK law as a critical reason for the UK rising the rankings.

Researchers referenced Ministers' decision to incorporate the EU's General Data Protection Regulation into UK law as a critical reason for the UK rising the rankings.

The German authorities have recently developed specific regulations on IT security requirements. According to them [Directive 2015/2366/EU] the basis of the technical standards on authentication and communication developed by European Banking Association (EBA) under section 98 of Directive 2015/2366/EU:

"The personalised security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers. Payment initiation service providers do not necessarily enter into a contractual relationship with the account servicing payment service providers and, regardless of the business model used by the payment initiation service providers, the account servicing payment service providers should make it possible for payment initiation service providers to rely on the authentication procedures provided by the account servicing payments service providers to initiate a specific payment on behalf of the payer."

This statement concerns only banking, but it can be implemented for cloud services.

To sum up, we can see the tendency of regulation the authentication process in the banking, but not the cloud services. That is why it is needed to implement the best solutions to protect user's theft while the authentication process into the clouds.

4. Authentication process threats in the cloud technologies

The authentication process becomes not useful in case of users' lost, forgeting or damaging their authentication key, which depends on the authentication method. It has a significant impact on the safety of the authentication system in the clouds.

CSA asked experts to compile professional opinions on the most significant security issues within cloud services [CSA]. The experts think that the primary reason for the lousy tendency for cracking the cloud services is higher strategic decisions by executives in cloud adoption.

According to the report, the main threats are data cracking, lack of access management, insiders, misusing the cloud services, vulnerabilities in the shared technologies. A data violation might be the primary objective of a targeted attack or just the result of human error, application vulnerabilities, or poor security practices that are used in the system. The enterprises' cloud-based data may have the material or monetary worth to different parties for different reasons as well.

A data violation is an incident where confidential information is broken, viewed, stolen or used by an unauthorized user.

Cloud service providers reveal a set of application programming interfaces (APIs) that customers use to maintain control over the cloud technologies and interact with them. The security of these underlying APIs determines the safety and accessibility of main cloud services. If providers are not careful, an attacker with access to the key can cause a denial-of-service or rack up fees on behalf of the victim [Insecure API]. They need to be done or planned with a protecting purpose against the accidental and malicious make an effort to achieve the circumvent policy.

System vulnerabilities mean dupable bugs in programs that attackers can use to gain access to the computer system in motivation to steal the data, taking control over the network or interrupting service operations. Weaknesses over the components of the operating system like Kernel, system libraries and application tools that put the security at high risk.

Everybody who connected to the cloud service management system can read, modify, and delete data; issue control level and management operations; monitoring the data in transit or release ransomware that is convinced to go from a reliable source. In the end, insufficient identity, credential, or critical controlling can enable unauthorized access to data and possible extremely unfortunate damages to all parties.

Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still are used and successfully here. Cloud solutions are no exception. These types of stealing are widely used here as well. If an attacker gains access to the user's credentials, they can monitor the activities and transactions in the account, change data, misuse confidential information and redirect the customer to unlawful web-pages.

All types of attack can be successful because of the weak authentication algorithm. Authentication protocols differ from the protection methods they provide against assaults [Hickey K. Dark cloud].

The insider threat is a real potential risk, as it can be anyone who works for the company. An insider, such as an auditor, can access potentially sensitive information. An everyday basis is attacking the employer's cloud applications and functions. Revenge might motivate these people. Overall, the 'inside job' is responsible for most cloud computing security woes. Enterprises have to become proactive in finding solutions to their security threats to protect their sensitive information [INSIDER THREATS].

Data stored in the clouds can be lost for reasons other than cyber attacks. The data can be physically removed from the storage server or building, where this server is located, can be destroyed by earthquake, fire, etc. However, these type of catastrophes can be prevented, and protection methods have to be implemented.

Enterprises often struggle with identity management as they try to set aside permissions appropriate to the employees' job. The crucial mistake is that they forget to remove user access when a job position changes or a user leaves the organization at all. Such behavior can lead to different bad consequences.

One more critical threat is lack of diligence. It is about the confirmation of the information that has been submitted to the service providers and the validation of the given back information by the services providers. It creates with all benefits a lot of risks [CLOUD SERVICE VENDOR].

As well as ransomware attacks are successful, so are Denial-of-service (DoS) attacks. More cloud services come into usage, the more DDoS attacks on them will become more ordinary and daily [As cloud use grows].

In conclusion, we can see that many threats caused a lot of risks. Some of them are data losing, damaging the buildings, appearing the insiders, misusing the confidential data, the personal discredit, cracking the network, unauthorized transactions. And based on these risks, it is possible to find the best method to protect the authentication process in the cloud services.

5. Methods of protection and authentication protocols

According to the identified risks, it is crucial to determine the methods of protection.

Considering that cloud service is using over the Internet, the most proper method is having the user turning extra to the traditional username and password pair. From this point, it is recommended to use one or more of the techniques as:

- Physical token;
- Digital certificate;
- Biometry;
- SMS password confirmation.

Encryption is a well-known technology that can keep under control the access, and its use has been demonstrated its ability to provide data useless to those who do not have the key. It is exemplified by the uselessness of encrypted information and hashed passwords to cybercriminals. The cryptography is an excellent power in protection data, and it is standardized [The Impact of a Data Breach].

Multifactor authentication systems – smartcard, one-time password (OTP), and phone authentication. This form of authentication helps address password theft, where stolen passwords enable access to resources without user permission. Password theft can manifest in common network attacks, such as “pass the hash.”

The Cloud Security Alliance has developed the most effective ways of the cloud protections. Here are some methods [DEVELOPMENT OF AUTHENTICATION PROTOCOLS]:

1. Data storage. Encryption

Encryption is one of the most effective ways to protect data. The provider gives access to the data must encrypt the customer information stored in the data center, as well as, if not necessary, irrevocably deleted.

2. Data protection during transmission

Encrypted data during transmission should be available only after authentication. Data cannot be read or modified, even if accessed through unreliable nodes. Such technologies are quite known, providers have long used algorithms and reliable protocols AES, TLS, IPsec.

3. Authentication

Authentication - password protection. For higher reliability, tokens and certificates are often used.

4. Isolation of users

Using an individual virtual machine and a virtual network. Virtual networks must be deployed using technologies such as VPN, VLAN, and VPLS.

Credentials and cryptographic keys must not be implanted in the source code or are given a share in public facing repositories such as GitHub because there is a significant chance of the misuse. Keys need to be appropriately hidden and secured; that is why a well-secured public key infrastructure (PKI) is required in order to ensure key-management activities are accomplished.

As the lack of diligence is a significant threat to the cloud solutions, there are some points to fix the situation [CLOUD SERVICE VENDOR]:

- Asked to prove the cloud service provide their reliability using the free trial version and ceasing from storing essential data.
- Reading the feedback from customers of the chosen service provider.
- Visit service provider site
- Regular providing the audits (compliance and security)

As for Denial-of-Service attacks, the only solution is to use automated tools to spot and defend the core cloud technology from this type of attacks. Further, the tools will become better, that will help to prevent such threats.

Now, modified versions of old protocols are used around the world, which makes it possible to improve the algorithms already developed and make them more cryptoresistant.

In recent years, enterprises want to get convenient and flexible information infrastructure through the cloud computing. However, information security issue of cloud computing has been one of the thresholds for the enterprise to adopt cloud computing. The enterprises began to deploy a private cloud to solve the cloud security issues. SSL virtual private network (VPN) gateway is a solution for the enterprise to access private cloud services securely. There are two main types of SSL VPN gateway, i.e., SSL Portal VPN and SSL Tunnel VPN.

IT administrators may integrate existing account of active directory or lightweight directory access protocol (LDAP) to SSL VPN gateway. Therefore, IT administrators can easily configure SSL VPN gateway to control the different groups of users which can use what kind of resources and applications. Besides, SSL VPN gateway provides a mobile one-time password (MOTP) to enhance security authentication.

Here are some methods of protection the cloud attacks while implementation of the protocols:

- request-response, timestamps, random numbers, identifiers, digital signatures have to be used;
- the administrator must establish the result of the authentication, e.g., exchange secret session key will be used for the connection with the user;
- the new authentication must be initiated during the reconnection.

As we are passing our data through the internet, we need to check that our data is secure not only in storage but also when it is transmitted through different channels. The network security parameters should be considered to achieve the goal. Firewall and gateways should be set up appropriately to avoid hackers entering and stealing valid data. We also need to make use of secure communicating layers and protocols to prevent data loss by violator. The expert can use the secure socket layer for communicating. Other options include HTTP over SSL which is called HTTPS. Another alternative to HTTPS is secure HTTP (SHTTP). Depending on what kind of security mechanism we need to deploy for our application, we should decide on the communication protocols considering its pros and cons.

Here are some methods of protection the cloud attacks while implementation of the protocols:

- request-response, timestamps, random numbers, identifiers, digital signatures have to be used;
- the administrator must establish the result of the authentication, e.g., exchange secret session key will be used for the connection with the user;
- the new authentication must be initiated during the reconnection.

There are other methods of authentication:

1. Server SSH/RDP proxy.
2. Two-factor authentication.
3. Kerberos.
4. LDAP and SAML.
5. Single Sign-On.

Finally, it has demonstrated the need for secure connection to add more methods of the authentication. Besides, users have to use the most convenient tool for the accessing on their devices.

6. Approbation of research results

The results can be used for creating new authentication algorithms. That consider all strong sides in the current authentication solutions and strengthen the weak parties.

The research shows a massive number of vulnerabilities, and with the development of the cloud, it is clear that weaknesses will increase.

7. Conclusions

We can see the tendency of regulation the authentication process in the banking, but not the cloud services. That is why it is needed to implement the best solutions to protect user's theft while the authentication process into the clouds.

The research has demonstrated the need for secure connection to add more methods of the authentication. Besides, users have to use the most convenient tool for the accessing on their devices.

Frist, it is easily perceived that simple password authentication should be supplemented in other ways. Second, with the advent of a large number of devices, users need to use a reliable way to authenticate these devices. Finally, each user, developer, and provider have to care about the security of the data they are using.

In this article, the method of protection must contain not only practical usage but consider all weaknesses of the platform – the cloud solutions. The research shows that there are o lot of vulnerabilities that have to be fixed. Since the hackers for unauthorized access to the stored data can use them.

REFERENCES

1. Cloud Standards Customer Council. Security for Cloud Computing Ten Steps to Ensure Success Version 2.0. – 2015. – 35p.
2. Filimoshin V. Yu. Davletkireyeva l.z.: Secure authentication without using https. - International Journal of Open Information Technologies (2017) 7, 17-23.
3. Hickey K. Dark cloud: Study finds security risks in virtualization / Kathleen Hickey // Technology, Tools and Tactics for Public Sector IT. - 2010 - № 3 — p. 3-5
4. Khazhieva A. S.: Principles of information protection in the cloud. - Achievements of science and education (2017) 6(19), 14-16.
5. Lozhnikov P., Sulavko A., Buraya E., Pisarenko V.: Authentication of Computer Users in Real-Time by Generating Bit Sequences Based on Keyboard Handwriting and Face Features. - questions of cyber security (2017) 3(21), 24-34.
6. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing / National Institute of Standards and Technology / Rebecca M. Blank. – Gaithersburg: NIST, 2011. – 286 p.
7. Vishniakou U.A., Ghondagh Saz M.M.: Authentification models in cloud computing for mobile applications with intellectual support of choice. – Doklady BGUIR. - Electronic resource: https://www.bsuir.by/m/12_104571_1_112204.pdf#page=82, 2017.
8. Winkler J.R. Securing the Cloud. 1st Edition / Vic (J.R.) Winkler. - US : Syngress, 2011. - 314p.
9. Cloud Standards Customer Council. Security for Cloud Computing Ten Steps to En-sure Success Version 2.0. – 2015. – 35p.
10. Filimoshin V. Yu. Davletkireyeva l.z.: Secure authentication without using https. - In-ternational Journal of Open Information Technologies (2017) 7, 17-23.
11. Hickey K. Dark cloud: Study finds security risks in virtualization / Kathleen Hickey // Technology, Tools and Tactics for Public Sector IT. - 2010 - № 3 — p. 3-5.

12. Khazhieva A. S.: Principles of information protection in the cloud. - Achievements of science and education (2017) 6(19), 14-16.
13. Lozhnikov P., Sulavko A., Buraya E., Pisarenko V.: Authentication of Computer Users in Real-Time by Generating Bit Sequences Based on Keyboard Handwriting and Face Features. - questions of cyber security (2017) 3(21), 24-34.
14. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing / National In-stitute of Standards and Technology / Rebecca M. Blank. – Gaithersburg: NIST, 2011. – 286 p.
15. Vishniakou U.A., Ghondagh Saz M.M.: Authentification models in cloud computing for mobile applications with intellectual support of choice. – Doklady BGUIR. - Elec-tronic resource: https://www.bsuir.by/m/12_104571_1_112204.pdf#page=82, 2017.
16. Winkler J.R. Securing the Cloud. 1st Edition / Vic (J.R.) Winkler. - US : Syngress, 2011. - 314p.
17. Douglas Paris-White. Five features of information security every cloud platform should provide. - IBM Cloud Blog, February 6, 2018 – [access: https://www.ibm.com/blogs/bluemix/2018/02/five-fundamentals-cloud-security/]
18. Eric O'Neill. Why the future of cybersecurity is in the cloud? - Eric O'Neill. - 27 April 2018 – [access: https://www.cloudcomputing-news.net/news/2018/apr/27/why-future-cybersecurity-cloud/]
19. ICT. Online Authentication Threats and Attacks. - ICT.govt.nz. Authentication standards - 21/09/2016
20. Krutz, Ronald L. and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. - Indianapolis, IN: Wiley, 2010. - 179p.
21. Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview. – IBM Security, June 2017 – 34 p.