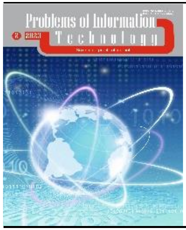

Available online at www.jpit.az

14 (2)
2023

Security issues and solution mechanisms in cloud computing systems: a review

Rashid G. Alakbarov

Institute of Information Technology, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

rashid.alakberov@gmail.com

0000-0002-7566-371X

ARTICLE INFO

http://doi.org/10.25045/jpit.v14.i2.02

Article history:
Received 02 March 2023
Received in revised form 13 April 2023
Accepted 03 May 2023

Keywords:
Mobile cloud computing
Mobile hardware
Security
Cyber-attacks
Computing and memory resources
Cloud computing
Privacy
Virtual machine
Cloud services

ABSTRACT

The recent rapid development of cloud technologies has encouraged its widespread use by individual mobile users, private organizations and public institutions. Mobile users and organizations deploy their data on cloud servers and use it. Connections to cloud servers are realized over the Internet, which makes data transmitted over the network vulnerable to various types of attacks. Although numerous security solutions have been proposed for data security in cloud computing systems, the security of provided services remains an actual problem for both cloud users and cloud service providers. The article provides a general survey of security and privacy issues in cloud computing systems, and reviews various types of attacks and possible threats, as well as protection methods and available solutions against such attacks, and proposes mechanisms.

1. Introduction

Cloud computing systems are a new generation of computing technology providing solutions to problems that require high computing and memory resources by using resources distributed over a network. Ensuring data security in cloud computing systems is crucial. These systems store important user data on cloud servers, and the security and confidentiality of this data depends entirely on the cloud providers. Without proper authentication and security algorithms, problems arise in protecting the customers' and organizations' data from attackers. Cloud computing systems provide companies and users with access to computing and storage resources and software applications via the Internet. Despite all the benefits as flexibility, scalability, and convenience, cloud computing users also face security challenges that require serious solution mechanisms. Security and ivacy issues are considered to be the main factor that may prevent further widespread use of cloud computing. Mobile user and enterprise data are stored and processed on cloud servers. They use wireless communication technology to communicate with mobile devices and between servers of cloud computing systems, which generates many security problems [Gayathri, et al, 2014; Gopichand, 2016]. Security issues in mobile cloud computing (MCC) systems combine security issues arising in cloud computing, mobile computing, and wireless networks. In MCC, data is stored and processed on cloud servers. Thus, to ensure data integrity, confidentiality and availability issues in MCC systems, it is important to analyze security-related problems in different parts of the system, that is in mobile devices, network infrastructure, cloud servers and software applications. This article extensively explores the problems related to security and privacy arising in different parts of MCC (mobile devices, network infrastructure, cloud servers, etc.) and offers mechanisms for solving the security issues arising in them.

2. Related studies

(AlZain, et al, 2012; Cachin, et al, 2009) propose storing the data on several distributed servers to solve security and privacy issues in cloud computing system. The proposed model divides the data into blocks; each block is encrypted and stored in the storage system of independent cloud servers. Even if an attacker tries to access one of the cloud storage systems and destroy the data, the other cloud storage system will remain secure, which will ensure the data integrity to be restored. (Shankarwar, et al, 2015) addresses privacy issues by dividing the encrypted data of mobile users into subparts and storing them in different cloud servers. (Popovic, et al, 2010) notes that multiple virtual machines (VMs) created on a cloud server pose security threats to each other. It proposes a model to prevent threats from VM. In order to ensure data security in the network environment, a multi-level architecture is proposed for solving mobile applications in cloudlets close to the user (Kovachev, et al, 2012). (Portokalidis, et al, 2010) develops a model to detect threats on mobile devices (smartphones) using the CloudAV platform. The proposed method reduces the transmission load in the network and a 30% reduction in energy consumption is detected, and the proposed method improves data security in mobile devices. (Kim, et al, 2012) studies the security and privacy problems caused by malware in cloud computing systems. These malwares infect VMs created on cloud servers and quickly spread to other VMs. This causes the data loss on cloud servers. It is suggested to use the Cloud AV platform to solve the problem. (Alhenaki, et al, 2019) outlines security in cloud computing, analyzes various types of attacks, and offers protection methods and solutions for such attacks. (Gupta, et al, 2016) realizes an overview of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks and possible protection mechanisms to be implemented in a cloud computing environment. It discusses many issues and problems in cloud environment protection against DoS attack. The study proposes mechanisms to combat the problem of DDoS attack and other similar attacks in cloud computing environment. (Subramaniam, et al, 2016) reviews the conceptual architecture of cloud computing systems, the main security criteria for cloud computing, the security risks for the cloud and the existing solutions to the security problems in cloud computing with its mitigation and presents recommendations. (Rajeshkuma, et al, 2020) extensively analyzes three main aspects of security issues in cloud systems, i.e., privacy, integrity, and availability, and proposes approaches to increase and protect security capabilities. (Hassan, et al, 2016) comprehensively examines available studies on cloud computing security problems and solutions. Finally, the authors propose a model for cloud computing security protection. The article provides a comprehensive overview of security issues for various factors affecting cloud computing. Security issues in public and private cloud systems are analyzed. In addition, it proposes a three-level security architecture to address security issues (Singh, et al, 2016). (Ahmed, et al, 2023) discusses cloud computing security threats, challenges, strategies and solutions. The architectural model of cloud computing is reviewed and security issues are analyzed and solutions are proposed. (Shajan, et al, 2021) highlights the main cyber threats facing cloud computing systems. It also indicates the countermeasures that the cloud provider should take to ensure the cloud environment security and protection from attacks. (Odun-Ayo, et al, 2021) examines current trends in cloud security and presents suggestions for further research. Algorithms are proposed for solving security problems in the system. The article provides a general overview of cloud technologies and discusses its models and features. Models for emerging security-related problems and solutions are proposed (Kalaivani, et al, 2021).

3. Data security and privacy protection in mobile cloud computing

The security issues of mobile cloud computing cover a wide spectrum and affect all components of cloud computing system (i.e., mobile devices, network infrastructure, cloud servers, etc.). Security issues include security and privacy of personal data, security of cloud services, risk resistance of cloud infrastructure, conducting security audits, registration (accounting) of resource allocation, authentication of users and devices, etc. Completeness, privacy and accessibility come to the fore in ensuring data security.

Data security and privacy protection. Cloud service providers must inform users about the procedures to ensure the security and privacy of user data deployed in the cloud. Users seriously concern about the privacy and security of their data located on cloud servers. The issue of data security and privacy protection is one of the reasons preventing mobile users and organizations from deploying their data on cloud servers (relying on cloud providers).

Cloud provider employees typically have access to user data. They try to steal or misuse data, which seriously affects the reliability of the cloud platform. These people can use unauthorized operations to harm the organization’s reputation. They can easily get passwords, encryption keys and data and can affect the cloud provider’s confidence reputation by creating security issues. In order to prevent them, the risk of security breaches and data theft can be reduced by regularly conducting security monitoring in cloud computing systems. Cloud providers are responsible for ensuring the data security on cloud servers. Although the data is initially stored in certain cloud servers specified by the cloud providers, these data can be transferred from one place to another place in terms of security, and in this case security issues come to the fore (Shahzad, et al, 2013; Diaby, et al, 2017).

Security measures in mobile cloud computing typically require protection procedures such as encrypting downloaded mobile application applications and data, and authenticating mobile devices and users. This entails additional costs in terms of more resources, processing time and energy consumption to perform security functions at a high level. Below the threats to data security and privacy in mobile cloud computing (Alakbarov, 2021; Prasanga, 2016):

- transferring data over the network to cloud servers creates the risk of losing control over the data. Users do not know where their data is actually stored, how it is processed, and this does not allow them to fully control the stored data;
- security vulnerabilities arise when insufficiently updated software is used in the cloud infrastructure. This can make them a target for a variety of infrastructure attacks, including malware, phishing and DDoS attacks, which can lead to data loss;
- a security risk may arise in the use of virtual machines due to the lack of physical isolation of virtual machines created on one server;
- data in the cloud may not be sufficiently protected, especially when it is transmitted over the network, which creates risks of hacker interception of data in communication channels during transmission of users’ personal and confidential data over the network;
- theft and loss of mobile devices;
- failure to use encryption and decryption keys effectively;
- lack of standards to ensure data completeness;
- and so forth.

A number of safety procedures are used in MCC to solve the above-mentioned problems:

Access control. Strict access control policies define who can access the data and applications in the cloud and how to access.

Using encryption software. If users have sensitive information such as passwords, credit cards, it is important to use encryption software to protect (hide) these from other network users. Therefore, every organization should have own encryption mechanism.

Updating software. Software is often constantly evolving. The software you use should include the latest modifications and updates.

Using antivirus software. Any system should include antivirus software to detect malicious code and remove or block them without causing any harm to the system. With the help of these programs, malicious activities of malware can be prevented.

Using anti-spam software. By using anti-spam software, it is possible to eliminate spam that attackers use to intrude users' email systems.

Using filters and software gateways. Downloadable malware can be disabled through a gateway and the potential risks are considerably reduced.

Multi-level authentication. Using multi-level authentication increases the security rate by requiring not only passwords, but also additional confirmations such as codes on mobile devices.

Monitoring and incident detection. Implementing monitoring systems can track anomalies and suspicious behavior, helping to identify potential threats earlier.

Security audit. Audit logging enables tracking user activities and verifying their compliance with security policies.

The architecture of MCC systems differs from traditional computing systems, making it vulnerable to a wider range of attacks. This is primarily due to the following reasons (Becher, et. buy, 2011):

Limited resources of mobile devices. The technical parameters (computing and memory resources) of mobile devices are less compared to personal computers. This prevents the necessary security software (antivirus, etc.) from running on mobile devices, leaving them vulnerable to attacks. For example, running monitoring tools (packet analysis and intrusion detection tools, security software, etc.) overloads a mobile device's computing resources and reduces its uptime due to rapid power depletion.

Using multiple connections to store and process data on cloud servers. Data from mobile devices is often uploaded to and stored on cloud servers. Moreover, software applications are processed on cloud servers. Storing data and code in multiple locations (e.g., mobile device, cloudlet, and cloud servers) makes them vulnerable to attacks.

Using mobile network infrastructure. In mobile cloud computing, users have the option to transfer their data to the cloud servers of some cloud providers that offer mobile services and process them there. By analyzing the characteristics of cloud network infrastructure (such as cloud topology, bottlenecks, communication channels, etc.), attackers can identify vulnerabilities and launch sophisticated attacks targeting them. Thus, mobility in cloud architecture creates a new set of threats (Huan, 2010).

4. Security threats in different parts of mobile cloud computing systems

Security threats occurring in different MCC components can be structured into the following groups (Gopichand, 2016 Rayapuri, 2018; Thoreau, do. buy, 2021; Alakbarov, etc. al, 2018):

I. Physical threats to mobile devices
II. Threats to network infrastructure
III. Threats to software applications
IV. Web-based threats
V. Threats to cloud servers

I. Physical threats to mobile devices. Memory resources, operating systems, software, communication links of mobile devices are threatened by attackers through various attacks. In particular, some attacks (threats aimed at mobile device memory resources and operating system security) directly impact the security of mobile devices in the cloud. Mobile devices have become an integral part of our lives and are widely used for personal and business purposes. Being small and light also makes mobile devices more likely to be stolen or lost. Consequently, if the user loses the mobile phone, if it is not blocked in advance with a PIN code or password, the person who gets the mobile phone can access the user's personal data.

II. Threats to network infrastructure. Mobile devices connect to cloud servers using Internet network infrastructure. Attacks on data by hackers are primarily realized on the network infrastructure. Network threats emerging in mobile cloud computing are as follows (Ahmed, et. Al, 2023; Kumar et al. buy, 2013; Thoreau, do. al, 2021):

Use of unsafe networks. If the user connects to an unknown network at airports, restaurants, shopping centers, etc. using Wi-Fi communication channels, which are not highly secured, an attacker can install malware on the user's mobile device without their knowledge.

Wi-Fi Sniffing is software designed to capture data transmitted over a network and decode the data into a human-readable format. It is developed to retrieve data from communication channels in wireless networks. Hackers can use this software to steal user data and monitor network activity.

Denial of service. The hacker continuously sends numerous data to the cloud servers, overloading them, which prevents users from using the cloud services. Distributed denial of service (DDoS) can be an example.

Data theft in the network inter-node connection (session). In order to gain unauthorized access to information or services on a computer, attackers use a trusted connection (session) key to steal data.

III. Threats to software applications. It may affect the integrity and confidentiality of data and applications. An attacker modifies the functionality of a mobile application by locating one of the malicious programs (virus, worm, trojan, etc.) into the mobile application. Threats to software applications are listed below:

Malware is a program that damages (disables) software on a user's system or performs malicious actions without the user's knowledge. For example, an attacker sends a malicious software attachment to a user's mobile device, enters the system, and then, at the command of the attacker, can send unwanted messages to people on the user's contact list, or can get the user's personal information and use it for other purposes (Rosenfeld, et. al, 2010).

Application software. Most mobile phone users use a mobile management system to process application software by synchronizing the collaboration between the phone and the personal computer. This method is often done via FTP. In FTP, the username and password are transmitted over the network and stored in a configuration file. Using FTP, an attacker gains unauthorized access to mobile phones by capturing user name and password, which allows the leakage of personal data and the deliberate data deletion from computer systems on the same network.

Spyware. These programs secretly collect information about a person or organization and gain control over the device without the user's knowledge. It is mainly used to track the Internet user behavior (which resources he/she uses, who he/she communicates with, etc.) and to store the collected data.

Interference with sensitive (weak) applications. Even the smallest flaw in the application can cause the entire software to be hacked. Such vulnerabilities allow an attacker to hack sensitive data, stop the service operation, etc. To avoid problems due to such small mistakes, making regular adjustments to the system helps to prevent such situations.

Threats caused by unlicensed software. Use of unlicensed software may subject the company to legal fines (costs). Simultaneously, attackers can use vulnerabilities in these programs to prevent the usual system operation. Therefore, regardless of whether the software used is licensed or not, vulnerabilities in the software used to prevent data theft should be regularly handled.

IV. Security of web-based applications. Threats to web-based software applications include:

Phishing - one of the types of internet fraud. Hackers realize this by sending emails and text messages on behalf of well-known brands and banks in order to capture the user's confidential information (login and password, bank card details, etc.). These messages often redirect the user to a fake website or requests the user to present protected information as credit card information, bank details, etc. This information is then used by an attacker to steal personal information or funds.

Browser security - a form of malware code that attempts to exploit a vulnerability in the operating system to compromise browser security and to change browser settings without the user's knowledge. The user uses a browser to interact with webpages. Browsers use the SSL protocol to ensure the protection of user identification information. However, hackers always create security problems by using the sniffing package installed on the intermediate host.

SQL injection attack - one of the most accessible ways to hack database-driven websites and applications. A hacker injects malicious SQL code into the data to gain unauthorized access to the database and obtain confidential information. SQL injection attacks modify SQL queries, use gaps (vulnerabilities) in application software to inject malicious code, thereby accessing unauthorized data and changing its contents.

V. Security threats in cloud servers. The goal of a cybercriminal is to capture useful information and use it for their own purposes. Attacks can be carried out by illegal cloud users or employees of cloud operators. On the other hand, the attacker intends to make the cloud platform unusable. For example, cloud services can be unusable by organizing DOS attacks [Donald, et. al, 2013]. Therefore, the cloud provider must use existing security technology to ensure that the service is available. When placing user data on cloud servers, the user must be ensured that such data cannot be accessed by anyone except those authorized by the providers. The cloud user must be guaranteed about the security and privacy of data stored on cloud servers. (Sarrab, 2015).

Security policies and procedures must be implemented by providers to ensure data security. Policies related to access control, authentication procedures, encryption, content and general communication security should be developed and certain measures should be taken to enforce them (Monjur, et. al, 2014).

Cloud computing systems use virtual machines generated on cloud servers to provide users with computing and storage resources. Therefore, the security of virtual machines generated on cloud servers is one of the main issues. Attackers must protect the operating systems of virtual machines from malware and viruses that attack physical servers. Cloud providers are responsible for the security of virtual machines. Security threats to cloud servers include:

Security issues in virtualization. Virtualization refers to the process of generating a virtual version of a computer. Virtualization technique helps the user to use cloud services efficiently. Providers enable users to use virtual machines on cloud servers to process their tasks. Cloud providers use virtualization to provide mobile users with multiple virtual machines created on a single server. The main advantage of using a virtual machine is that the providers create machine samples with different technical parameters according to the requirements of the users through the hypervisor and organize its use. This process leads to many security problems such as unauthorized access in MCC, mutual attack between virtual machines, etc. (Christodorescu, et. al, 2009).

Flooding attacks. The hacker continuously sends uninterrupted requests to the cloud server about the need for additional resources. Since cloud servers have scalability features, they provide the hacker with the resources according to requests. This, in turn, causes the system to run out of resources and the system cannot serve real users.

Security issues in uploading data to cloud servers. Mobile users have no control over the process of uploading their data to the cloud servers and they must access the cloud servers when uploading the data. This enables any user to gain unauthorized access to uploaded data. The uploading process is performed by employees of cloud providers, which may compromise the integrity and privacy of uploaded content. In MCC, the user uses the mobile network to upload data to cloud servers, but in this case, a risk of intruders accessing the data during the upload arises. The main problem with uploading is the disruption of accessibility caused by failure (blocking) of the mobile device during upload. Furthermore, when uploading data, if the data contains any malicious codes, it will affect the privacy and security of the mobile user's data (Rahul, et. al, 2017).

5. Mechanisms for solving security problems in various components of mobile cloud computing

The following mechanisms and recommendations are proposed for solving security problems arising from the threats to the various components of mobile cloud computing mentioned above (***data, network, cloud servers, virtual machines, cloud resources, mobile devices, etc.)***:

1. Data security mechanisms in MCC. It is recommended to use the following mechanisms to ensure data security in MCC:

Using secure communication protocols. It is recommended to apply secure communication protocols such as SSL/TLS and VPN to ensure secure data transfer between the mobile device and cloud servers.

Storing data on distributed multi-cloud servers and using encryption methods. If the data is grouped into segments, and each segment is encrypted and stored in multi-cloud storage, even if fraudsters try to breach one of the cloud storage systems, the other cloud storage system will remain safe, which will ensure the data integrity to be restored.

Block-based Sharing Scheme (BSS). It is a cryptographic method that logically groups the data into blocks. Each block is encrypted and has decryption capabilities to return the data to its original form. This method provides better security by simply reducing the computing. Moreover, it ensures the privacy and integrity of data (Abdul, et. al, 2014).

Using the ciphertext policy attribute-based encryption (CP-ABE) algorithm. Attribute-based encryption is a type of public-key encryption that encrypts the user's private key and the ciphertext using attributes. Here, confidential data is required to be encrypted from the mobile device to the transmission to the cloud servers. Data must be stored in the cloud in encrypted text form to prevent access to sensitive data. Encryption will reduce the speed of data usage, thus the emphasis is on the efficient processing and parsing of the ciphertext. The proposed CP-ABE algorithm for ciphertext encoding provides access control in the MCC environment and allows the mobile user to perform data processing quickly (due to reduced encryption and decryption operations). This ensures data protection from unauthorized access.

Data partitioning model. When uploading software applications to cloud servers, it is recommended to use data partitioning techniques to prevent theft of user's personal data. This technique consists includes three steps: in the first step, the data is grouped into sensitive and non-sensitive segments, in the second step, sensitive data is processed on the mobile device, and in the third step, non-sensitive data is processed on cloud servers. The results obtained on the cloud server and mobile devices are combined with the mobile device itself and the final result is presented to the user (Dhanya, et. al, 2015).

TinMan model. This algorithm ensures the security of the confidential user data even when the mobile device is stolen. Because it ensures secure uploading and privacy of software applications to cloud servers. In this concept, sensitive data is separated from regular mobile apps, then uploaded to the cloud and stored on a trusted node. VMs of cloud servers are used to create this node. In this method, SSL (Secure Socket Layer) and TCP protocols are used in the process of downloading and obtaining confidential information for security purposes (Yubin, et. al, 2015).

Methods for ensuring security when offloading software applications to cloud servers. The CMReS (Cloud Manager-based re-encryption scheme) cryptographic method is proposed to be used in the download, which protects the software attachments. This method uses data encryption, decryption, and re-encryption for stronger security during offload, and these processes are controlled by the client (Ko, et. al, 2011).

2. Mechanisms for ensuring the security of the mobile network infrastructure. The following mechanisms are proposed for solving the problems in ensuring the mobile network infrastructure security:

Network traffic monitoring. Network traffic monitoring can help identify any suspicious activity or unauthorized access to the network infrastructure. This can be done using intrusion detection firewalls and network traffic analysis tools.

Regular security audits. Conducting regular security audits may detect any gaps or vulnerabilities in the system. Audits can be performed by internal or external auditors, and the results obtained should be used to improve the organization's security posture.

Implementing business continuity plans in the event of a disaster. System business continuity plans should be developed and tested to ensure that the organization can continue to operate in the event of a disaster or system outage. Plans should include data backup and recovery, migration to alternative infrastructure, and relationships with stakeholders.

Using network segmentation. Network segmentation involves grouping a network into smaller subnets to reduce attack chances and limit the spread of potential breaches. This can be achieved by using firewalls, VLANs, or virtual private networks (VPNs).

Regular safety training for employees. Employees can be the weak link in the safety chain, consequently it is important to conduct regular safety training to educate them about the ways to reduce risks. This should include training on password hygiene, social engineering and phishing attacks.

3. Data security mechanisms on cloud servers. Performance and reliability of the MCC system are important for both users and operators. Above all, cloud services incorporate existing security solutions, including VPN technology, authentication and authorization, encryption and other technical means, and can organize a continuous service available against various threats such as DoS attacks and data theft. Furthermore, cloud providers can use full backup and disaster recovery plans to restore user data in the event of a DDoS or flood attack. In this manner, it can improve the quality of service and gain the trust of users.

Encryption is required during the process of offloading software from a mobile device to cloud servers and processing. Data should be stored in the cloud in encrypted text form to prevent leakage of confidential information. However, encryption will reduce the speed of data usage, accordingly the encryption of the text should be done using efficient methods (Jiang, et. Buy, 2019). The following mechanisms are proposed to ensure security in cloud servers:

Using data encryption. Proper encryption and decryption methods must be used to protect the data security on a network connection. For this, it is recommended to use secure protocols such as SSL/TLS and strong encryption RSA algorithms (Lee, et al, 2016).

Using reliable cloud provider. It is important to choose a reliable cloud provider with experience in security. The provider must have strong security controls, undergo regular audits and assessments, and provide transparent reports on its security posture.

ThinAV cloud-based solution algorithm. This algorithm uses two components: the mobile client software and the ThinAV server. Once the mobile client application offloads the application to the cloud server, it also allows the application to be offloaded to the ThinAV server, if the ThinAV server detects the presence of malware in the software application, it sends the result to the mobile client software, which deletes the infected files (Chris, et. al, 2012).

Using the Secure Data Sharing in Clouds (SeDaSC) algorithm. This method involves three parts, i.e., the user, the cryptographic server, and the cloud.

- user submits the data (list of group members) to the cryptographic server;
- cryptographic server encrypts data using a symmetric key after receiving data; the key is gouped into two parts: one for group members and the other for access control (for the cryptographic server);
- cryptographic server stores the split data in the cloud. When a group member wants to download data, it sends the request along with the symmetric key to the cryptographic server. Once the request is received, the cryptographic server authenticates the user to verify whether he/she is a valid member, and then allows him/her to decrypt and upload the data to the cloud for storage (Mazhar, et. al, 2015).

4. Recommendations for ensuring security in virtualization. Several mechanisms are proposed to overcome the security problems arising in virtualization:

Secure Mobile Cloud Platform (SMOS). This platform allows users to securely clone (duplicate) the operating system and applications in a VM in the cloud. Hardware virtualization allows the isolation of data and applications from the operating system on a mobile device to ensure data security, which provides a higher level of data security (Hao, et. al, 2015).

Using a security platform. This platform includes two protocols: a secure VM startup protocol and a data protection protocol on a domain-based storage system. A trusted VM initialization protocol is used before deployment with a guest VM, and then a domain-based storage data protection protocol is used to ensure data privacy (Nicolae, et. al, 2017).

5. Recommendations for securing mobile cloud software applications. The following protocols are recommended for securing mobile cloud applications.

Secure Mobile Cloud (SMC) protocol. This protocol enables the components in the network to communicate securely with each other and ensures the integrity of applications (installation, update, etc.) on mobile devices [Popa, et. a, 2013].

A hybrid attribute and re-encryption protocol. These protocols help secure mobile cloud applications. These two protocols use attribute-based encryption, group key, and re-encryption techniques. Attribute-based encryption shares key generation duties between the mobile device and the trusted entity. A group key provides a private key for a group that is used only by group members, and that private key is re-encrypted (Tysowski, et. al, 2013).

A secure mobile application model. The primary goal of this security model is to provide secure authentication, communication, and migration across mobile device and cloud components. The proposed model is used to solve the security problems arising in the execution of the mentioned processes. The main components of this model are: device manager, cloud manager and software manager (Zhang, 2014):

- device manager locates software applications within network components and chooses a secure path for communication.
- cloud manager allocates resources and stores information about software applications (computing capabilities, channel bandwidth, etc.).
- software manager installs and runs software applications on different cloud nodes.

Strict, Observable, Verifiable Data and Execution (STOVE) model for unreliable applications. This model helps unlicensed software run securely by isolating its components from other mobile device applications and the operating system. It prevents fraudsters to gain unauthorized access to data or applications. Users can run structured insecure programs on their systems using the STOVE model, ensuring that these programs will not harm or gain unauthorized access to their system (Tan, et. al, 2014).

6. Recommendations for securing data on mobile devices. A number of proposals are presented to ensure data security on mobile devices (physical threats, malicious programs, cloud-related threats, etc.). The following mechanisms are proposed to eliminate security-related problems in software applications used on mobile devices:

Solutions for physical threats. To ensure security on mobile devices, it is proposed to use OpenFlow for data transfer between the mobile device and the cloud, thus ensuring security during the process. In order to prevent the data misuse on the mobile device if the mobile user loses the device, Google offers a special service that if the device is lost/stolen, the data inside the device can be remotely deleted and also locked.

Malware prevention solutions. Malware attacks can be prevented by using security software either in the cloud or on mobile devices. It is recommended to use CloudAV anti-malware software. CloudAV is a new concept for mobile device malware detection in cloud intranet (Liu, et. al, 2013).

Software troubleshooting. Updating and installing any software on mobile devices should be realized carefully. Correspondingly, the user should verify the authenticity of the software while installing or downloading it.

Ensuring user awareness. Nowadays, most of the cyber-crimes or hacks are caused by the negligence or lack of knowledge of the users. To prevent attacks, the user should avoid using non-essential connections (Toro, et. buy, 2021). For example, it is recommended to turn off Bluetooth after use and avoid using public Wi-Fi. It is also important to be careful when transferring data from foreign devices. These can significantly reduce the spread of malware.

Solving the problem of mobile device data storage. The problem of safe storage of mobile device data can be performed through cloud storage services, data encryption and encryption key protection through Trusted software.

Cloud-based solutions. The limited resources of mobile devices prevent the implementation of advanced security monitoring systems that work with personal computers. Due to resource limitations, antivirus software cannot be enabled on mobile devices to prevent malware. Therefore, cloud-based security software is used on smartphone devices. Hence, security software is offloaded and used on servers in the cloud to protect against malware.

Using the Secloud security monitoring platform. It is proposed to use the Secloud security monitoring platform to ensure the security of mobile devices (smartphones) in the network environment. The Secloud platform emulates (imitates) a registered smartphone device within a designated cloud and secures the device by continuously transmitting its logins and network connections to the cloud. The system uses three components such as mobile client agent, emulator, and proxy server. A mobile client agent is software that runs on a mobile device, the emulator creates VMs of mobile devices on cloud servers and hosts them on a proxy server. The proxy server monitors the tracking of the mobile device’s network traffic. When the emulator detects security problems, it either informs the mobile client agent, which deletes the infected files, or informs the proxy server to disrupt the attacker's network connection (Zonouz, et. al, 2013).

6. Conclusion

Cloud computing systems provide numerous Internet services to mobile users and organizations, however, simultaneously, they cause security problems in data transmission over the network. Solving these problems requires a complex approach and the application of various security mechanisms. The correct implementation of these measures allows for more effective protection of data and programs deployed in the cloud, and increases the level of user trust in cloud services. This article extensively analyzed the data security, privacy, data integrity, cyber-attacks, etc. in MCC systems. It explored the threats to the security and privacy of MCC data and highlighted a number of security procedures used to ensure the problem solution. Security threats arising in various components of MCC systems (mobile devices, network, cloud servers, software applications, web-pages, etc.) were analyzed in details and grouped. Moreover, different types of attacks and possible threats related to security and privacy in different parts of cloud computing systems, as well as protection methods and available solutions against these attacks, were reviewed and mechanisms were proposed.

References

Abdul, N., Laiha M., Mazhar A., Shahaboddin Sh. (2014). "BSS: Block-based Sharing Scheme for secure data storage services in mobile cloud computing" The Journal of SuperComputing, vol. 70, no. 2, pp. 946-976. DOI: 10.1007/s11227-014-1269-8.

Ahmed B.U, Amin R., Mehmood M., Aldabbas H., Alharbi M.T. & Albaqa N.. (2023). "Cloud Security Threats and Solutions: A Survey", Wireless Personal Communications, vol. 128, pp. 387-413. DOI: 10.1007/s11277-022-09960-z

Alakbarov R.G. (2021). "Mobile cloud technologies: current state, problems and security issues", Information Technology Problems, vol.1, s. 15-32. DOI : 10.25045/jpit.v12.i1.02

Alakbarov R.G., Alakbarov O.R. (2018)."Security and privacy issues in mobile cloud computing", Information Technology Problems, №1, s. 92-102. DOI : 10.25045/jpit.v09.i1.09

Alhenaki L., Alwatban A., Alahmri B., Alarifi N. (2019). "Security In Cloud Computing: A Survey", International Journal of Computer Science and Information Security, vol.17, no.4, pp. 67-90.

AlZain M., Pardede E., Soh B., Thom J. (2012). "Cloud computing security: From single to multiclouds", 45th Hawaii International Conference on System Science (HICSS), pp. 5490-5499.

Becher M., Freiling F., Hoffmann J., Holz T., Uellenbeck S., Wolf C. (2011). "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices", In: Proceedings of the 2011 IEEE Symposium on Security and Privacy, SP'11, Oakland, IEEE Computer Society, Washington, pp. 96-111. doi:10.1109/SP.2011.29

Cachin C., Keidar I., Shraer A. (2009). "Trusting the cloud", ACM SIGACT News, vol. 40, no. 2, pp. 81-86. DOI: 10.21522/TIJAR.2014.SE.19.01.Art009

Chris, J. David B., John A. (2012). "ThinAV: Truly Lightweight Mobile Cloud-based Anti-malware", Twenty-Eighth Annual Computer Security Applications Conference, pp. 209-218. DOI: 10.1145/2420950.2420983.

Christodorescu, M., Sailer R., Schales D., Sgandurra D., Zamboni D. (2009). "Cloud security is not (just) virtualization security: a short paper" In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, CCSW'09, Chicago, ACM, New York, pp. 97-102. doi:10.1145/1655008.1655022

Dhanya N., Kousalya G. (2015). "Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing" International Symposium on Security in Computing and Communication, vol. 536, pp. 45-53. doi.org/10.1007/s11276-022-02920-2

Diaby, T. Rad B.B. (2017). "Cloud Computing: A review of the Concepts and Deployment Models", I.J. Information Technology and Computer Science, vol. 6, pp. 50-58. doi:10.5815/IJITCS.2017.06.07

Donald, A., Oli S., Arockiam L. (2013).Mobile cloud security issues and challenges: A perspective, International Journal of Engineering and Innovative Technology, vol. 3 (1), pp. 401–406.

Gayathri M.R., Srinivas K. (2014). "A Survey on Mobile Cloud Computing Architecture, Applications and Challenges", International Journal of Scientific Research Engineering & Technology, vol. 3, no. 6, pp.1013-1021

Gopichand, M. (2016). "An Overview of Security and Privacy Issue in Mobil Cloud Computing Environment", International Journal of Advanced Researc in Computer Science and Software Engineering, vol. 6, no. 5, pp. 779-784.

Gupta, B., Badve, O. (2016). "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment." Neural Computing and Applications, 28(12), pp.3655-3682. DOI:10.1007/s00521-016-2317-5

Hao, Z. Tang Y., Zhang Y., Novak E., Carter N., Li Q. (2015). "SMOC: A secure mobile cloud computing platform", in Computer Communications (INFOCOM), IEEE Conference on, pp. 2668-2676. DOI:10.20944/preprints201912.0079.v1

Hassan N., Ahmed H. (2016). "A survey of Cloud Computing Securitychallenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), vol. 14, no. 1, pp. 52-58

Huan, L. A. (2010). "New form of DoS attack in a cloud and its avoidance mechanism", In: Proceedings of the 2010 ACM Workshop on Cloud Computing Security, CCSW'10, Chicago, ACM, New York, pp. 65-76. doi:10.1145/1866835.1866849

Jiang, X. Kong W., Jin X., Shen J. (2019). "A Cooperative Placement Method for Machine Learning Workflows and Meteorological Big Data Security Protection in Cloud

Computing", In International Conference on Machine Learning for Cyber Security, Springer, Cham, pp. 94-111. https://doi.org/10.1007/978-3-030-30619-9_8

Kalaivani A., Sangeetha S. (2021). "Cloud computing data security challenges and algorithms to protect security issues", Journal of Hunan University（Natural Sciences, vol. 48, no. 12. pp. 2312-2323.

Kim T., et al. (2012). "Monitoring and detecting abnormal behavior in mobile cloud infrastructure", IEEE Network Operations and Management Symposium, pp. 1303-1310.

Kovachev D., Klamma R. (2012). "Framework for Computation Offloading in Mobile Cloud Computing", International Journal of Artificial Intelligence and Interactive Multimedia, vol. 1, no. 7, pp. 6-15. DOI:10.9781/ijimai.2012.171

Ko S., Jeon K., Morales R. (2011). "The HybrEx model for confidentiality and privacy in cloud computing", In: Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing, HotCloud'11, Portland, USENIX Association, Berkeley, pp. 1-5.

Kumar R. Rajalakshmi S. (2013). "Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems", In 2013 International Conference on Computer Sciences and Applications, IEEE, pp. 663-669.

Li, H. Shou G., Hu Y., Guo Z. (2016). "Mobile edge computing: Progress and challenges", In 2016 4th IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud) IEEE, pp. 83-84. DOI:10.1109/MobileCloud.2016.16

Liu, F., Shu P., Jin H., Ding L., Yu J., Niu D., Li B. (2013). "Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications", IEEE Wireless Communications, vol. 20, no. 3, pp. 14-22.

Mazhar, A. Revathi Dh., Eraj K., Samee U., Athanasios V., Keqin Li L., Albert Y. (2015). "SeDaSC: Secure Data Sharing in Clouds", IEEE Systems Journal, vol. 11, no. 2, pp. 1-29. DOI: http://doi.org/10.1109/JSYST.2014.2379646

Monjur A., Hossain M. (2014). "Cloud computing and security issues in the cloud", International Journal of Network Security & Its Applications, vol. 6, no. 1, pp. 25-36.

Nicolae, P. Christian G., Antonis M. (2017.) "Providing User Security Guarantees in Public Infrastructure Clouds", IEEE Transactions on Cloud Computing, pp. 1-15.

Odun-Ayo I., Ajayi O., Misr S. (2018). "Cloud Computing Security: Issues and Developments", Proceedings of the World Congress on Engineering, vol. , pp. 1-7.

Popa, D. Cremene M., Borda M., Boudaoud K.. (2013). "A Security Framework for Mobile Cloud Applications", Eleventh Roedunet International Conference, pp. 1-2. DOI: 10.1109/RoEduNet.2013.6511724

Popovic K., Hocenski V. (2010). "Cloud computing security issues and challenges", MIPRO, Proceedings of the 33rd International Convention, pp. 344-349.

Portokalidis G., Homburg P., Anagnostakis K., Bos H. (2010). "Paranoid Android: versatile protection for smartphones", Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), pp. 347-356. DOI:10.1145/1920261.1920313

Prasanga, H. (2016). "Security Issues of Mobile Cloud Computing", Independent Study Final Report. pp. 1-7.

Rahul, N., Nishi W. (2017). "Survey on Security issues of Fog Computing" International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 10, pp. 15731-15736. DOI: 10.15680/IJIRCCE.2017. 0510009

Rajeshkumar V. Patel, Dhaval Bhoi, Chandrashekhar S. Pawar., Rajeshkumar V. (2020). "International Journal of Scientific Research in Computer Science", Engineering and Information Technology, vol. 6, no. 4, pp. 48-58

Rayapuri, B. (2018). "A Survey of Security and Privacy in Mobile Cloud Computing", Masters Theses. 3406. Western Michigan University, pp. 1-55.

Rosenfeld K., Karri R. (2010). "Attacks and defenses for JTAG", IEEE Des. Test, vol. 27, no. 1, pp. 36-47. doi:10.1109/MDT.2010.9

Sarrab M. (2015). "Mobile Cloud Computing: Security Issues and Considerations" Journal of Advances in Information Technology, vol. 6, no. 4, pp. 248-251.

Shahzad A. Hussain M. (2013). "Security Issues and Challenges of Mobile Cloud Computing", International Journal of Grid and Distributed Computing, vol. 6, no. 6, pp. 37-50. http://dx.doi.org/10.14257/ijgdc.2013.6.6.04

Shajan A., Rangaswamy Sh. (2021). "Survey of Security Threats and Countermeasures in Cloud Computing", United International Journal for Research & Technology, vol. 2, no. 7, pp. 201-207

Shankarwar M., Pawar A. (2015). "Security and privacy in cloud computing: A survey", Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), ser. Advances in Intelligent Systems and Computing. Springer International Publishing, vol. 328, pp. 1-11

Singh S., Jeong Y., Hyuk Park J. (2016). "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications, vol. 75, pp. 200-222 DOI:10.1016/j.jnca.2016.09.002

Subramaniam. T.K, Deepa B. (2016). "Security Attack Issues and Mitigation Techniques in Cloud Computing Environments", Int. J. UbiComp, vol. 7, no. 1, pp. 1-11.

Tan J., Gandhi R., Narasimhan P. (2014). "STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications", IEEE Sixth International Conference on Cloud Computing Technology and Science, pp. 644-649. DOI: 10.1109/CloudCom.2014.116pp

Toro, M., Muhammad N, Shu'aibu A., Garba M., Abdulaziz A., Musa K. (2021). "Security, Privacy Issues and Solutions of Mobile Cloud Computing", United international journal for research & technology, vol 2, no. 7, pp. 112-117.

Tysowski P., Hasan M. A. (2013). "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds", IEEE Transactions on Cloud Computing, vol. 1, no. 2, – pp. 172-186. DOI: 10.1109/TCC.2013.11.

Yubin X. Yutao L., Cheng T., Mingyang M., Haibing G., Binyu Z., Haibo C. (2015). "TinMan: Eliminating Confidential Mobile Data Exposure with Security Oriented Offloading", Tenth European Conference on Computer Systems, vol. 27, pp. 1-16. DOI: 10.1145/2741948.2741977.

Zhang Y. Su S., Wang Y., Chen W., Yang F. (2014). "Privacy-assured substructure similarity query over encrypted graph-structured data in cloud", Journal of Security and Communication Networks, vol. 7, no. 11, pp. 1933-1944. https://doi.org/10.1002/sec.907

Zonouz S.Z., Houmansadr A., Berthier R., Borisov N., Sanders W. (2013). "Secloud: A cloud-based comprehensive and lightweight security solution for smartphones, Journal of Computer and Security, vol. 37, pp. 215-227. doi: 10.1016/j.cose.2013.02.002.