E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 17-07-2023
Accepted: 22-08-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 1; Issue 1; 2023; Page No. 511-516

Study of mobile cloud computing security and its challenges

[1]Suchit Kumar Vyas and [2]Dr. Satish Kumar

[1]Research Scholar, Department of Electronics and Communication Engineering, Himalayan University, Arunachal Pradesh, India
[2]Assistant Professor, Department of Electronics and Communication Engineering, Himalayan University, Arunachal Pradesh, India

DOI: https://doi.org/10.5281/zenodo.13950280

Corresponding Author: Suchit Kumar Vyas

Abstract

The rise of cloud computing has significantly impacted software organizations and the design of software architecture. As cloud computing and mobile internet continue to evolve, mobile cloud computing is emerging as a new application model. This model combines three key technologies: mobile computing, cloud computing, and wireless technology. Mobile cloud computing has become a crucial and advanced technology today, yet mobile devices still face several challenges. These include issues related to storage, security, privacy, and connectivity. Mobile cloud computing offers resources and services from the cloud to mobile devices, supporting the development of specialized mobile applications. However, data outsourcing and synchronization over the Internet introduce increased risks to security and privacy. This research paper explores mobile cloud computing, its security challenges, and proposes potential solutions.

Keywords: Mobile cloud computing, security, wireless technology

Introduction

Mobile cloud computing has become a crucial area for communication and storage in today's technology landscape. It leverages cloud computing and the internet, integrating three core technologies: mobile computing, cloud computing, and wireless networks. This combination enhances computing and storage capacities, providing a better experience for mobile device users. Cloud computing supports resource-based operations via the internet, broadening the computing capabilities available on mobile devices. This field represents a new frontier in information technology, promising numerous benefits in the future. Cloud computing integrates diverse technologies to offer services, platforms, and infrastructure to various users and organizations. Mobile cloud computing builds on this by combining cloud computing with mobile devices and wireless technologies, facilitating seamless connectivity across environments. As technology advances, an increasing number of users are uploading various types of data, including sensitive information, to the cloud. This raises significant concerns about data security and privacy. The advantages of mobile cloud computing are realized when cloud computing is applied to mobile environments, utilizing mobile device storage to deliver benefits to users. Figure 1 illustrates the components of Mobile Cloud Computing. Recent advancements in this field, which operates as a network of computers and applications, have spurred considerable research potential within cloud computing. Mobile cloud computing addresses the limited storage capacity of mobile devices by storing data on the cloud and accessing it via mobile applications. While there are many applications and benefits of mobile cloud computing, the risks associated with data storage, such as potential theft, are also significant. This paper will explore these aspects in detail.

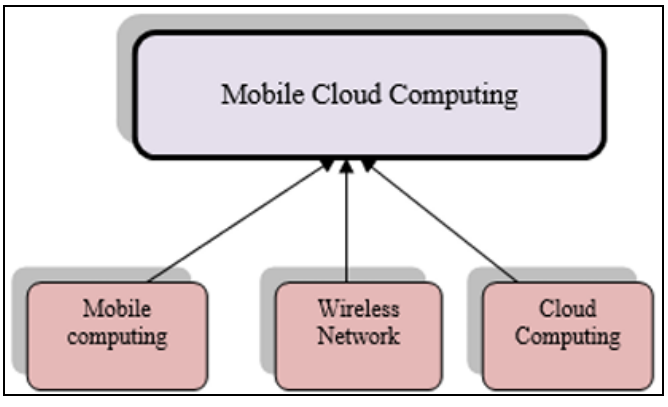

Fig 1: Mobile cloud computing

MCC architecture

Mobile devices, including laptops, PDAs, and handheld gadgets, can access cloud services via wireless access points (WAP) or mobile networks. Base Transceiver Stations (BTS) or satellites are used by mobile devices to connect to mobile networks. These entities manage the functional interfaces and connections between mobile devices and mobile networks. In order to provide a wide range of mobile network services, including AAA (Authentication, Authorization, and Accounting), they transmit the requests and data from mobile users to Base Station Controllers (BSC), which are further connected to the Mobile Switching Center (MSC).

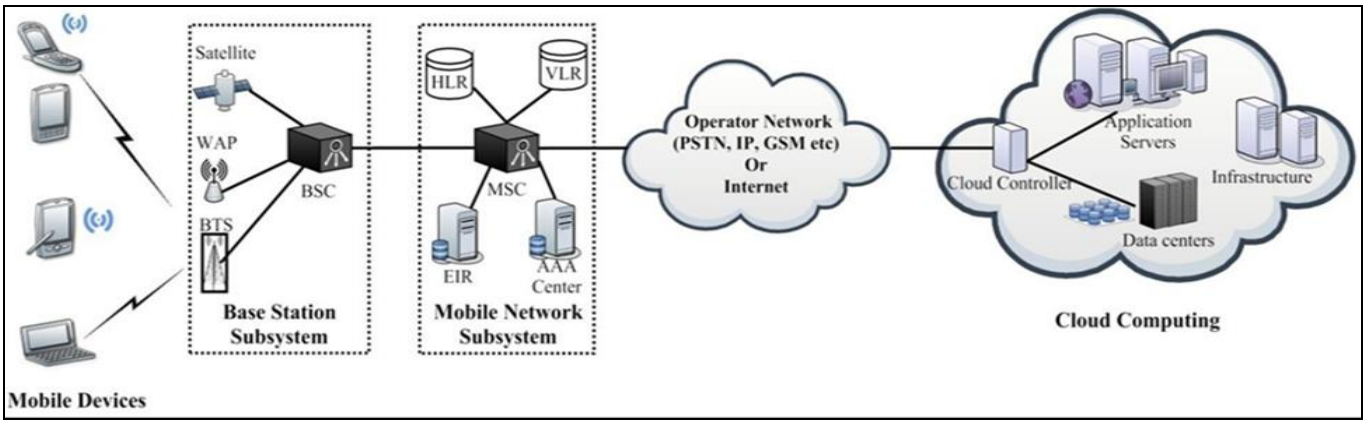

Fig 2: MCC architecture

These BSCs rely on subscriber data stored in databases as well as information from the Home Location Register (HLR), Visitor Location Register (VLR), AAA center, and Equipment Identity Register (EIR). The queries from the subscribers are subsequently sent over the Internet to a cloud. In a WAP scenario, mobile devices establish a Wi-Fi connection with the access points, which in turn establishes a connection with the Internet Service Providers (ISPs) to provide Internet access. Due to its low latency and energy consumption, Wi-Fi-based connectivity is more effective than mobile network GSM, GPRS, 3G, LTE, and 4G connections. Utilizing virtualization, service-oriented architecture, and ubiquitous computing, cloud controllers within the cloud establish connections with data centers and application servers to handle requests and deliver the corresponding cloud services to mobile users.

MCC Applications

One of the technologies that is spreading the fastest in history is mobile service. MCC is advantageous for a number of applications and has had a significant impact on the global market.

People's lives have been transformed by mobile commerce (m-commerce), which offers a variety of applications like online tickets, banking, and mobile purchasing. These programs had to contend with issues like poor battery life, limited bandwidth, intricate mobile architecture, and security vulnerabilities. To get over the aforementioned problems, MCC combines cloud and mobile commerce apps.

The integration of e-learning and mobility, known as mobile learning or m-learning, is not without its difficulties, including poor transmission rates and expensive mobile device prices. By using the cloud for huge storage and powerful computation, they can be avoided.

Unlike traditional medical applications, mobile healthcare (m-healthcare) enables mobile users to efficiently access medical resources. The limitations of mobile medical applications, such as minimal storage capacity, security, and data reliability, are solved by the availability of on-demand services on the cloud.

Because mobile gaming (m-gaming) demands a lot of processing power and graphic rendering, the game engine module is offloaded to the nimble cloud servers.

Cloud computing can be used to develop and host mobile apps. In order to save repetitive development and maintenance efforts, mobile apps that operate simultaneously on various mobile platforms—such as Windows, Android, and Apple iOS—may rely on the cloud for storage, processing complex calculations, and fault tolerance.

MCC challenges

While moving to the mobile cloud is an alluring trend, there are a few more considerations that need to be made. These are as follows:

- **Heterogeneous environment:** Mobile nodes connect to the cloud using a variety of network interfaces and radio technologies, such as WLAN, CDMA, WCDMA, GPRS, and WiMAX, in heterogeneous networks where MCC is implemented. Handling wireless connectivity-which must meet specific MCC criteria such always-on connectivity, on-demand scalability, and energy efficiency of mobile nodes-becomes problematic due to heterogeneity.
- **Low bandwidth:** Given that the number of cloud users is growing at an alarming rate, bandwidth is a major obstacle. As a result, mobile nodes that are close to one another, inside a business, office, etc., or that are interacting with the same content must share and distribute the limited bandwidth fairly. The upcoming technologies that can get around this bandwidth restriction are 4G and femtocells.
- **Security and privacy concerns:** The MCC paradigm's success depends in large part on safeguarding user confidentiality and privacy from outside threats.

Protecting mobile devices from various security threats is more difficult than defending resourceful devices because of their resource constraints.

- **Identity:** Management and access control are necessary because cloud servers that are heavily virtualized and federated are not seen as reliable. Only authorized users should be able to access encrypted data thanks to these policies, which also require fine-grained access control.
- **Key management:** Data encryption using cryptography might show to be an effective means of guaranteeing confidentiality and safeguarding data prior to outsourcing data in the cloud. In an MCC setting, key management-that is, key creation, distribution, and monitoring-is a crucial component of data encryption.
- **Searchable encryption techniques:** These days, researchers are paying more attention to encrypted data on the cloud because it is encrypted before being outsourced to cloud servers.
- **Remote integrity check:** A significant security issue that is drawing attention from researchers is the design of effective remote integrity check methods for confirming the integrity of data stored in the cloud without downloading a copy of the data to a mobile device.
- **Context-aware apps:** Unleashing the power of MCC in the diverse environment towards unconstrained ubiquitous computing requires designing resource-efficient and context-aware applications to improve the quality of service. Monitoring the pertinent device data, such as location, capabilities, environment, user profiles, and preferences, is essential for optimizing mobile access and offering context-aware mobile services to various users.
- **Energy management:** Reducing energy consumption and improving the energy efficiency of mobile devices and the cloud are the main concerns in a mobile cloud environment. CSPs must leverage server consolidation, energy-efficient scheduling, and a thoroughly thought-out transmission protocol to do this while minimizing resource waste.
- **Live virtual machine migration:** It makes data center provisioning incredibly reliable and responsive possible. By distributing the load evenly among the datacenters, virtualization techniques are used to achieve this. The primary problem is how to securely and without any data loss move the entire virtual machine (VM) as it is in a matter of milliseconds from one server to another.
- **Availability:** Compared to the traditional CC paradigm, one of the main problems with MCC is service availability. In the MCC paradigm, there are many disconnections caused by node mobility, signal attenuation, network or link failures, and traffic congestion. Mobile users are unable to connect to the cloud for a service as a result of these disconnections. In the event of a disconnect, a mechanism must exist to enable mobile users to establish a cloud connection through nearby nodes.
- **Standard interface:** Because there are no standards, customers are hesitant to move their data centers to the cloud. It is also challenging to move or scale an application or data across several CSPs when portability and interoperability are lacking. In order to maintain a seamless connection between mobile users and CSPs, a standard interface is necessary, as the present web interface for communication between mobile users and cloud incurs greater overhead. In the near future, an effective interface may be made possible using HTML5 Web Sockets.

Security issues in MCC

Identification and authentication methods must be safe, dependable, and unrepudiated in order for MCC to proliferate widely. Despite the fact that cloud and mobile cloud computing offer a wealth of resources, security has become a barrier to their adoption. Numerous security risks, vulnerabilities, and potential attacks have been covered in this area.

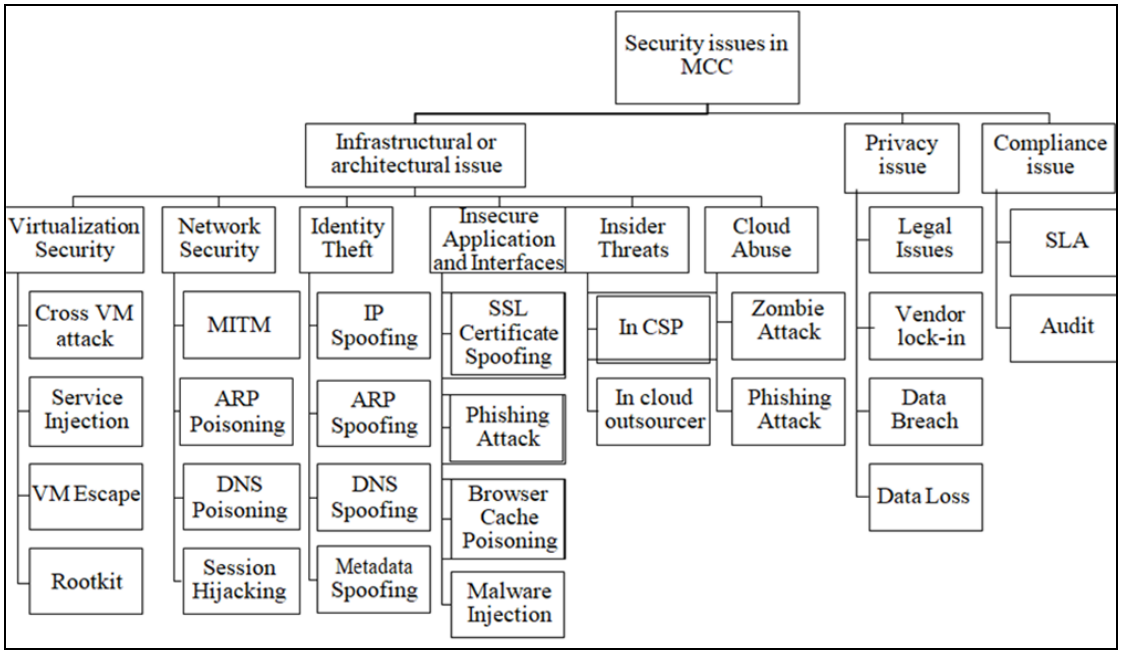

Fig 3: Security issues in MCC

Infrastructural issues

This component covers network security, data segregation concerns, insider threats, virtualization security, and administrative interface problems.

- **Virtualization security:** One of the key elements of cloud computing is virtualization, which enables sharing of on-demand services and the storing of data by different users via SaaS provider applications. In the event that tenants' data are improperly segregated both physically and application-wise, there is a substantial risk of data breach. Numerous hazards result from it, including isolation between different virtual machines operating on the same physical computer, cross-VM attacks, the introduction of malicious code into the program, and vulnerabilities in virtualization software known as hypervisors, which can be used to elevate privileges and get beyond authentication. For instance, weak software It is possible for guest machines to execute malicious code on the host computer or other guest machines while using Microsoft Virtual PC and Microsoft Virtual Server. Through the use of a VM Escape attack, a hacker can breach an isolation layer, execute a program with root access to the hypervisor, and gain access to the host's operating system and any other virtual machines that are executing on it. An attacker can obtain administrator-level access to a computer by using a rootkit, which is a collection of applications or tools, to break passwords or take advantage of flaws in hypervisors. Using virtual machine (VM)-based rootkits, an attacker can run malicious code that disables anti-malware software to avoid detection and take control of all virtual machines (VMs) operating on the physically infected machine. Robust isolation between virtual machines (VMs) and thorough hypervisor monitoring are necessary to prevent an attacker from inserting malicious code into a neighboring VM.
- **Network security:** It addresses setups and communications on networks. An attacker can take advantage of the cloud system and its resources by using techniques like Man-In-the-Middle (MITM) attacks, ARP poisoning, DNS poisoning, session hijacking, and other vulnerabilities present in Internet protocols including ARP, HTTP, and TCP. Strong network encryption solutions like SSL and TLS are necessary to defend against attacks of this kind since data is taken from a company and kept on cloud platforms.
- **A Man-in-the-Middle (MITM):** Attack, caused by improper SSL settings, allows an attacker to access data transfer between two parties, including data centers and virtual machines (VMs). Because ARP does not require proof-of-origin, a malicious attacker can use an ARP poisoning attack to reroute all incoming and outgoing traffic from other virtual machines to its own machine. By intentionally altering DNS cache material, a DNS poisoning attack deceives the domain name server (DNS) into sending traffic in the incorrect route. Customers using cloud services need to be sure that CSPs are protecting their DNS infrastructure in the right ways. In a session-hijacking attack, the attacker takes advantage of HTTP's incorrect session ID implementation to assume the user's identity and continue communication. One way to prevent such attacks is to encrypt traffic and use anonymous authentication. Firewalls and protocols need to be set up to give cloud environments the necessary level of security.
- **Identity theft:** This type of fraud involves someone assuming the identity of another person in order to get access to resources or obtain banking and other vital data. Identity theft can take many different forms, including phishing attacks, DNS spoofing, IP spoofing, ARP spoofing, and metadata spoofing. To launch an IP spoofing attack, an attacker gains the IP address of a genuine user, modifies TCP/IP packet headers to impersonate a trusted host, and conceals its true identity. This technique can be used to steal data, overwhelm targets with traffic, and take control of browsers. An attacker uses an ARP spoofing attack to bind their MAC address to the IP address of a valid virtual machine (VM) in a network. They then send spoof ARP messages, which cause data meant for the IP address of the legal host to be delivered to the spoofing VM that is connected to the same virtual switch. Malicious attackers can alter data-in-transit, obstruct traffic on a local area network (LAN), or obtain access to confidential information or network resources by using ARP spoofing. In a DNS spoofing attack, a malicious machine provides a virtual machine (VM) with fictitious DNS information, causing the VM's browse request to be diverted to a fictitious IP address that the attacker has generated in order to steal banking credentials. In order for someone to access services online, a Web services description language (WSDL) file holds metadata or descriptions about those services. With a metadata spoofing attack, hackers can alter a service's WSDL file during a service delivery period in order to steal data or insert harmful code. Phishing attacks involve an adversary creating a phony URL that looks just like the real Web application, tricking visitors into entering legitimate credentials and certificates. Financial Fraud Action UK estimates that financial fraud, which is primarily caused by identity theft, was £755 million in 2015—a 26% increase over 2014. Collins, a resident of Lancaster, Pennsylvania, was charged in 2016 with using phishing emails to obtain unauthorized access to over 100 Gmail and Apple iCloud accounts. Apple advised enabling two-factor authentication following this incident since passwords are easily cracked by hackers. Enforcing robust remote authentication and authorization protocols is necessary to gain access to confidential cloud data.
- **Insecure applications and interfaces:** CSPs depend on administrative interfaces for virtual machine management, deployment, coding, testing, monitoring, user access control, and configuration; programming interfaces for virtualized resource access and service provisioning; and user interfaces for investigating resources and tools made available by CSPs. Multiple security hazards can be introduced into an organization by weak APIs and user interfaces. According to a security analysis of Amazon and Eucalyptus' control interfaces by Somorovsky et al. [2020], both systems

are readily vulnerable to cross-site scripting (XSS) and signature wrapping attacks. Malware injection attacks, including SQL injection, OS injection, XSS injection, and LDAP (lightweight directory access protocol) injection attacks, are caused by flaws in the design and architecture of applications. By inserting malicious code into a service or malicious virtual machine instance, an adversary compromises a cloud system by potentially altering or blocking service functions. As a result, malicious services receive the legitimate requests that are diverted. An adversary may, for instance, substitute a malicious command for the security group name in the Amazon EC2 API. Through the use of SSL certificates, which the user's browser may verify, the SSL protocol enables secure communication between the user's browser and the server. Secure connection is established if the trusted CAs pre-listed in the browser vouch for the server's SSL certificate; if not, a warning is sent to the user. By pretending to be a trustworthy server and using an SSL certificate poisoning attack, it is possible to break an SSL secure connection and intercept private data. An attacker uses a Man-in-the-Middle (MITM) attack on a user's HTTPS session to replace cached material with malicious data in a browser cache poisoning attack. Such attacks can be prevented by solid authentication procedures, secure user interfaces, data validation checks, and access control policies.

- **Insider attack:** Organizations and CSPs typically place a greater emphasis on thwarting external threats than they do on internal intrusions. Given his allowed access to the system and his familiarity with both the network architecture and system security protocols, an insider attacker can cause significant damage to the network or system with ease. A malicious employee of the cloud provider or an employee of a company using cloud services could be considered an insider employee. Insider attack damage can be mitigated by having clear job descriptions and open employee management procedures.
- **Cloud abuse:** When cloud services are used maliciously, including for cracking encryption keys, distributing pirated software, or spreading malware to launch DDoS and phishing attacks, it is considered abuse. These activities are difficult to carry out with a regular computer. Such attacks can be avoided by doing enough validation and verification checks at the initial registration step and by continuously monitoring network traffic.

Benefits of mobile cloud computing

The benefits of mobile cloud computing offer a distinct advantage compared to traditional mobile computing. It presents numerous opportunities for research across various domains, including natural language processing, image processing, querying, multimedia, sensor data applications, and internet access sharing. Mobile cloud computing effectively alleviates the data storage constraints of mobile devices, enhances battery life, and provides technical features such as location awareness services. By leveraging mobile cloud computing, users and organizations can significantly expand their storage capacity. For instance, companies like Facebook, Amazon, and Flipkart store vast amounts of data in the cloud, demonstrating how cloud storage can accommodate substantial data volumes.

Table 1: Shows the benefits of Mobile Cloud Computing

Sr. No.	Drawback of Mobile Devices	Benefits of Mobile Cloud Computing
1	Storage Capacity is limited	Storage Capacity in Unlimited
2	Battery Life Issue	Battery Life is Increased
3	Sharing Data With another Devices is low	Accessing data on Demand and self-service.

Conclusion

In this paper, we explore the technology of mobile cloud computing and its associated security challenges. Mobile cloud computing offers significant benefits by integrating cloud services with mobile devices. The use of various applications on mobile devices is increasing daily, but sharing personal files, data, or information through cloud storage introduces substantial security and privacy concerns. Our study investigates current research trends and identifies key areas of interest in mobile cloud computing, with a particular focus on data security and user privacy. We review past research to understand the drawbacks, technologies in use, applications, and advantages of mobile cloud computing. Despite advancements, issues such as data security, data confidentiality, application security, and offloading security persist. This paper aims to address these ongoing challenges and suggests areas for future research, emphasizing the need to improve data security and privacy in mobile cloud computing.

References

1. Abolfazli S, Sanaei Z, Shiraz M, Gani A. MOMCC: Market-oriented architecture for mobile cloud computing based on service-oriented architecture. In: Proceedings of the IEEE International Conference on Communications; c2012. p. 8-13.
2. Ahmed-Nacer A, Samovar MAN. Strong authentication for mobile cloud computing. In: Proceedings of the International Conference on New Technologies for Distributed Systems; c2016. p. 1-6.
3. Brenner M, Wiebelitz J, Von Voigt G, Smith M. Secret program execution in the cloud applying homomorphic encryption. In: Proceedings of the IEEE International Conference on Digital Ecosystems & Technologies; c2011. p. 114-119.
4. Chow R, Jakobsson M, Masuoka R, Molina J, Niu Y, Shi E, *et al*. Authentication in the clouds: A framework & its application to mobile users. In: Proceedings of the ACM Workshop on Cloud Computing Security; c2010. p. 1-6.
5. Hwang K, Bai X, Shi Y, Li M, Chen WG, Wu Y. Cloud performance modeling with benchmark evaluation of elastic scaling strategies. IEEE Trans Parallel Distrib Syst. 2016;27(1):130-143.
6. Khan AN, Kiah MM, Madani SA, Ali M. Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. J Supercomput. 2013;66(3):1687-1706.
7. Mulay M, Surana R, Tibdewal Y. Enhanced security in multi-cloud using visual cryptography & secret sharing.

Int J Cybernetics Inf Technol. 2015;17(3):128-139.
8. Rahulamathavan Y, Phan RCW, Veluru S, Cumanan K, Rajarajan M. Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud. IEEE Trans Dependable Secure Comput. 2014;11(5):467-479.
9. Singh S, Sharma S. Improving security mechanism to access HDFS data by mobile consumers using middleware-layer framework. In: Proceedings of the IEEE International Conference on Computing, Communication & Networking Technologies; c2014. p. 1-7.
10. Thangadurai K, Devi GS. An analysis of LSB based image steganography techniques. In: Proceedings of the International Conference on Computer Communication & Informatics; c2014. p. 1-4.
11. Wang SC, Liao WP, Yan KQ, Wang SS, Tsai SH. Security of cloud computing lightweight authentication protocol. J Appl Mech Mater. 2013;284:3502-3506.
12. Yousef M, Nebozhyn M, Shatkay H, Kanterakis S, Showe LC, Showe MK. Combining multi-species genomic data for micro RNA identification using a naive Bayes classifier. J Bioinformatics. 2006;22(11):1325-1334.