RESEARCH & INNOVATION DIVISION
IJIST

Enhancing Security in Mobile Cloud Computing: An Analysis of Authentication Protocols and Innovation

Amna Shahzadi, Kashif Ishaq*, Naeem A. Nawaz, Ghulam Mustafa, Fawad Ali Khan
School of Systems and Technology, University of the Management and Technology, Lahore, Pakistan
***Corresponding Author**: Kashif Ishaq Email: kashif.ishaq@umt.edu.pk

Citation | Shahzadi. A, Ishaq. K, Nawaz. N. A, Mustafa. G, Khan. F. A, “Enhancing Security in Mobile Cloud Computing: An Analysis of Authentication Protocols and Innovation”, IJIST, Vol. 6 Issue. 2 pp 351-365, Apr 2024

Received | Feb 28, 2024, **Revised |** Mar 21, 2024, **Accepted |** Mar 29, 2024, **Published |** Apr 06, 2024.

Introduction/Importance of Study: Cloud computing is a model facilitating ubiquitous, convenient, and on-demand network access to a shared pool of computing resources, offering flexibility, reliability, and scalability .

Objective: This study investigates authentication mechanisms in Mobile Cloud Computing (MCC) to enhance security and address emerging challenges.

Novelty statement: Our research contributes novel insights into authentication protocols in MCC, offering solutions to security issues not previously addressed.

Material and Method: The study analyzed various authentication mechanisms in MCC using NIST evaluation criteria, considering their alignment with security needs and resource constraints.

Result and Discussion: Our findings underscore the importance of selecting authentication mechanisms that balance security and performance in MCC environments, highlighting the need for ongoing innovation in security measures.

Concluding Remarks: The study emphasizes the significance of robust authentication protocols tailored to MCC's unique security requirements for ensuring data integrity and privacy.

Keywords: Authentication protocols; Mobile Cloud Computing (MCC); Security; NIST evaluation; Innovation.

Introduction:

Cloud computing is a model facilitating ubiquitous, convenient, and on-demand network access to a shared pool of computing resources, offering flexibility, reliability, and scalability [1][2][3][4][5]. The primary objective of computing models is to enhance capacity, capability, and access to new software licenses dynamically, without the need for additional infrastructure investment [6]. Illustrative examples such as Google Apps, Gmail, Google Maps, and navigation applications exemplify cloud computing, accessible over the Internet. The pay-as-you-go paradigm inherent in cloud computing facilitates the development of diverse models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), catering to both developmental and business needs [7][8].

Security is particularly crucial for applications transmitting personal information and conducting financial transactions. In Mobile Cloud Computing (MCC), the challenge of data security is exacerbated as data transactions occur over unreliable wireless mediums between cloud and mobile devices. This paper focuses on a specific security aspect concerning accountability in both Cloud Computing (CC) and MCC, achieved through user authentication. Authentication, a process verifying the identity of individuals or objects like mobile devices, entails comparing provided credentials with those stored in a database, ensuring security and privacy, particularly for applications transmitting sensitive data to the cloud. Authentication poses challenges such as complexity in providing user credentials, multiple handshakes for verification, and delays. In MCC, authentication complexity escalates due to communication occurring over various wireless networks (Wi-Fi, 3G, 4G). Authentication delay is critical in MCC for real-time applications like online movie streaming and gaming. This paper discusses authentication techniques for both CC and MCC, filling a gap in existing research where studies typically cover either CC or MCC authentication exclusively. To the best of our knowledge, this paper is the first to comprehensively cover authentication techniques for both CC and MCC.

The mobile industry witnessed a significant milestone in 2017, with over 5 billion users globally, 3.7 billion of whom were from developing markets, marking a substantial increase in mobile subscriptions worldwide. By 2019, the total number of mobile users was forecasted to surpass 5 billion, with smartphone users expected to reach 50%, driven by advancements in both hardware and software technologies [9]. The integration of mobile and cloud computing offers numerous benefits but exposes data transmission to security threats [2]. Further, MCC represents a novel computing paradigm tailored to the resource constraints of mobile devices [10], leveraging ubiquitous wireless connectivity [11], mobile web technologies, location-based services and cloud computing [4]. In MCC, users prefer accessing services from online servers rather than installing software on individual mobile devices. This approach enables any mobile device to leverage data processing and storage capabilities provided by the cloud [12]. Mobile devices face many limitations including unpredictable internet connectivity, low battery life, limited processing power, less storage space, limited network bandwidth, and security vulnerabilities [8][13][14]. To mitigate these constraints computationally intensive and storage-demanding tasks are offloaded to the cloud networks, alleviating the burden on mobile devices.

Cloud computing offers numerous advantages to mobile users including streamlined integration, enhanced reliability and scalability, efficient load balancing, and access to abundant resources. Additionally, it promotes energy efficiency [10], facilitates auto resource provision and de-provision, utilizes virtualization technology, and enhances data storage capacity and processing power.

Literature Review:

The literature survey on authentication mechanisms in MCC explores the critical role of authentication in ensuring secure access to cloud resources amidst the evolving landscape of mobile technology. Shi et al. [15] introduce an implicit authentication system that captures user routines and habits, such as making phone calls or visiting specific places at similar times, to construct individual behavior profiles. During the initial learning phase, the system collects past user behaviors to create a user model. This model is then used to compare recent user behaviors, determining whether authentication is permitted. The comparison generates a probability-based authentication score, which adjusts based on new observed behaviors. Routine activities and typical tasks contribute positively to the score, while a decline to a predefined threshold prompts explicit authentication.

Sathish and Venkataram [16] propose the TBAS (Transaction-Based Authentication Scheme), an authentication method centered on mobile transactions. TBAS operates at the application level, leveraging intelligent agents to classify user behavior and the sensitivity of transactions. Mobile Cognitive Agents (MCA) gather user behavior data, while static agents (SCA) identify transaction sensitivity and select appropriate authentication processes based on security requirements. Witte et al. [17] introduce a context-aware mobile biometric system utilizing Support Vector Machine (SVM) technology. This system learns and evaluates contextual information captured from various behavioral biometric features, such as speech patterns, online signatures, and keystroke dynamics, via active and passive sensors. Environmental conditions are also considered to construct subject-specific context models, as they can impact biometric feature reliability. The system gathers extensive contextual data to build accurate user models, followed by a training phase where the data set describing the current context is classified using a probabilistic model.

Dandachi et al. [18] introduce an implicit authentication approach utilizing data captured from smartphone sensors and user behavior. This method operates at both hardware and software levels to furnish a complementary dataset for precise authentication decisions. By integrating information from multiple sources, this approach enhances authentication accuracy. The primary reliance is on four sensors: Orientation sensor, Accelerometer, Rotation Vector, and GPS, supplemented by behavioral data analysis including keystroke and touch gesture analysis. Data classification is performed using Support Vector Machine (SVM) machine learning due to its proven performance and accuracy. The authors assert that the classification error rate for SVM was deemed acceptable following the application of a filtering algorithm.

Hung et al. [19] propose an activity-based security mechanism tailored to support user activities in ubiquitous environments. This system is grounded in image identification, where the user and authentication system establish a secret agreement on image features. Upon entering their username, the system presents a set of images for the user to select relevant ones based on the context. The scheme encompasses an Authentication Manager and Authorization Manager. The Activity Recognition Manager (ARM) supplies activity information to the authorization service by gathering contextual data characterizing user activities. The Authentication Manager ensures robust yet lightweight user authentication across different devices, while the Authorization Manager determines permissions based on monitored user activities. Corradi et al. [20] introduce a model of context-based access control named Ubiquitous Computing Context-based Security Middleware (UbiCOSM). UbiCOSM utilizes context as a foundational element for specifications and enforcement processes. Contextual changes systematically impact permissions, with each context linked to a set of applicable permissions. Positioned atop the existing context-aware middleware called CARMEN middleware, UbiCOSM operates at a higher level, providing various facilities including identification, communication, migration, monitoring, resource discovery, directory, context management, and event registration/dispatching.

In cloud computing, confidentiality plays a crucial role in maintaining control over organizations' data stored across distributed databases. Integrity ensures that unauthorized individuals cannot tamper with or manipulate sensitive data stored in cloud servers. By safeguarding against unauthorized access (confidentiality), organizations can ensure the integrity of their information and systems. The primary objective of availability is to prevent unauthorized individuals from accessing shared data in cloud service providers at any time and from any location. Cloud servers must have the capability to continue operations even in the event of a security breach. Denial of Service (DoS) attacks, natural disasters, and equipment failures pose risks to availability.

Cloud computing is an internet-based technology that offers various services over the internet, significantly impacting the economy in terms of efficiency, scalability, energy, and cost reduction. A service refers to a method capable of providing functionalities in compliance with established rules. Cloud computing services can be categorized into three types: Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS), as outlined by Ikram et al. [4]. SaaS, situated in the top layer, offers on-demand applications, delivering software as a service via the Internet, examples include Google Docs, Zoho, and Microsoft CRM. SaaS resolves issues related to installing and running applications on the customer's end [19][21]. PaaS, an extension of IaaS, comprises the second layer, allowing users to rent database management systems, operating systems, hardware, design tools, and network capacity (hosting) via the Internet [22].

IaaS forms the bottommost layer, providing fundamental computing infrastructure components such as storage, CPU, and memory. It encompasses hosting, hardware provisioning, and basic services required for cloud computing execution. Infrastructure comprises the underlying physical components necessary for system operations, with certain challenges discussed by Sheikh et al. [32]. There are several other types of cloud services, including Monitoring as a Service (MaaS), Data Storage as a Service (DSaaS), Communication as a Service (CaaS), Business as a Service (BaaS), and Security as a Service (SecaaS). Cloud services can be categorized based on four different deployment models: private cloud, public cloud, hybrid cloud, and community cloud.

A private cloud is a cloud platform dedicated to a specific user or organization. Unlike the public cloud, where multiple providers may offer various layers, the entire stack (IaaS, PaaS, and SaaS) is managed by a single provider, providing access and control over applications, infrastructure, and middleware. Community cloud is a cloud model shared by various organizations supporting a specific community and may be operated by the organizations themselves or by a third party. Public cloud refers to a model that grants client access to the cloud through interfaces using mainstream web browsers, making it available to public users. It is the dominant model when cost reduction is a priority, although it is generally considered less secure than other cloud models. A hybrid cloud is a combination of two or more clouds (private, community, or public) that maintain separate entities.

While cloud computing offers numerous advantages such as low-cost storage and shared infrastructure, its inability to ensure data privacy and confidentiality poses significant risks. Various security and privacy issues have been addressed by implementing different models of privacy managers in cloud computing, aimed at reducing the risk of theft and misuse of shared information in Cloud Service Providers (CSPs). These techniques help provide security for sensitive and critical data in cloud models. Research by Behl (2011) has studied security approaches for cloud infrastructure and their weaknesses, aiming to implement a security strategy to enhance the security of cloud environments.

Almusaylim et al. [9] enlightened the key issues in MCC major issues surrounding MCC, with a focus on the challenge of protecting user privacy, particularly in relation to Location-Based Services (LBS). It addresses concerns regarding the offloading of user location data to cloud providers and the potential risks of unauthorized access and misuse by third parties. The paper examines the specific challenges faced by LBS in safeguarding user location privacy and the potential consequences of compromised data. Additionally, it analyses existing approaches and proposes solutions to enhance privacy protections in MCC. Hence, Authentication mechanisms are crucial in MCC to ensure the security and integrity of user interactions with cloud-based services. With the increasing reliance on MCC and the proliferation of mobile devices accessing cloud resources, robust authentication is essential to verify user identities and protect sensitive data from unauthorized access [23].

Objectives:

This paper provides a comprehensive survey of MCC and discusses the benefits and security challenges associated with it.

Materials and Method:

By examining existing research, methodologies, and emerging trends, the survey aims to identify the strengths, weaknesses, challenges, and opportunities in authentication for MCC. Key topics include biometric authentication, multi-factor authentication, adaptive authentication strategies, and their implications for ensuring the integrity and confidentiality of cloud-based services. Through this survey, readers will gain valuable insights into the complexities of authentication in MCC and its significance for cybersecurity, enabling informed decisions in the design and implementation of secure authentication mechanisms for cloud-based applications and services.

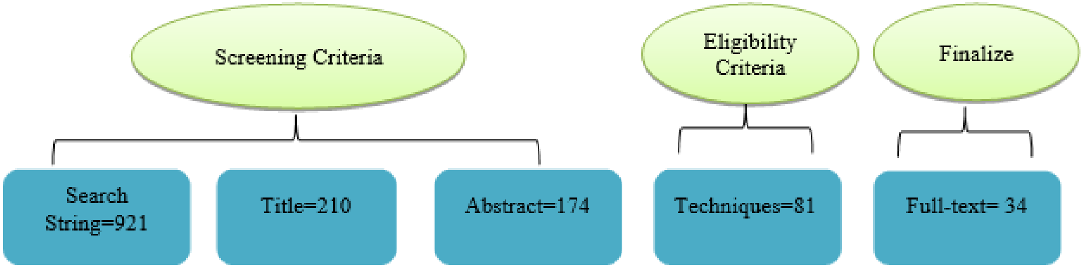

Figure 1: PRISMA diagram of Authentication mechanisms of MCC

Stages of Authentication Mechanisms in MCC:

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) diagram of Figure 1 of the literature review on authentication mechanisms in MCC involves some steps:

Identify Relevant Studies:

The process starts with a thorough exploration of esteemed academic databases, journals, conference archives, and pertinent resources to locate research on authentication mechanisms within MCC. This entails examining platforms such as IEEE, ACM, Hindawi, Springer, and Elsevier as well as NIST official reports.

Title-Based:

Utilize inclusion and exclusion criteria to sift through the identified studies, eliminating papers published before 2020 and those not in English. Select studies that specifically address authentication mechanisms within the MCC domain, while disregarding any irrelevant ones.

Data Extraction on an Abstract Basis:

Retain papers whose abstracts pertain to authentication mechanisms in MCC.

Synthesis and Analysis of Techniques:

Extract key data from the selected studies, such as study objectives, methodologies, findings, and conclusions related to authentication mechanisms in MCC.

Finalization:

Review and finalize the PRISMA diagram, ensuring that it accurately reflects the literature review process and provides a clear overview of the selected studies on authentication mechanisms in MCC. We have finalized approximately 34 papers for inclusion.

Results and Discussion:

Authentication Mechanisms:

When a mobile device establishes a connection and initiates communication over a wireless network, there is no guarantee of the secrecy of user credentials. Thus, optimizing the authentication process within a mobile cloud environment is essential. Tabrizchi et al [1] delve into authentication and identity management issues in MCC, highlighting two main technologies of security, access control, and user authentication. In MCC environments, where users interact with cloud resources through mobile devices over potentially insecure networks, Role-Based Access Control (RBAC) provides a flexible and scalable framework for managing access rights, mitigating risks associated with unauthorized access and data breaches. The RBAC is an access control technique that grants access to the user, based on their roles. User authentication techniques include Public Key Infrastructure (PKI), User ID and Password, Multi-Factor Authentication (MFA), and Single Sign (SSO).

A variety of authentication techniques serve as the backbone of the MCC framework, ensuring the authenticity of users. For instance, Fregly et al [23] present the Merkle Tree Ladder (MTL) mode, designed to reduce signature size impact in practical scenarios, especially within Mobile Cloud Computing (MCC) contexts. MTL mode condenses signatures, enabling their transmission in fewer bits between signers and verifiers. Through shorter condensed signatures and occasional longer reference values, MTL mode streamlines authentication processes while maintaining cryptographic resilience. The mode's effectiveness in reducing signature size impact, even with evolving cryptographic algorithms, underscores its potential for widespread adoption in MCC and other applications. Additionally, the author emphasizes the need for further specification development and integration considerations to fully leverage MTL mode's benefits across various authentication mechanisms. Overall, MTL mode offers a promising solution to optimize authentication efficiency and security in MCC environments and beyond

Likewise, ensuring confidentiality in the MCC environment relies on effective encryption measures [12][22]. Cao et al. [24] highlight the critical role of encryption in mobile computing, emphasizing its importance in safeguarding sensitive data during transmission and processing on mobile devices. In edge computing scenarios, where data processing occurs locally before transmission, encryption ensures confidentiality and mitigates the risk of unauthorized access. By employing encryption techniques, mobile computing environments can protect sensitive information from interception and maintain the security of mobile applications and services. Moreover, encryption secures communications between mobile devices and edge nodes, enhancing data privacy and overall security in mobile computing environments [14][17]. Overall, encryption plays a vital role in maintaining confidentiality and safeguarding sensitive data in the dynamic landscape of mobile computing [10].

Smart devices use MCC to do more things by sending some tasks to big computers on the internet. Ferrag et al. [22] conducted a comprehensive review of authentication schemes for smart mobile devices, categorizing threat models into five types and countermeasures into four categories. It analyses cryptographic functions, personal identification methods, and security analysis techniques used in these schemes. The surveyed schemes encompass biometric-based, channel-based, factor-based, and ID-based authentication. A comparative analysis is performed that, covers performance, limitations, and computational complexity. Identified challenging research areas include false data injection attacks, analysis of smart mobile devices under topology attacks, group authentication, and key agreement security in 5G networks.

Moreover, AlAhmad et al. [3] highlight critical security issues in Mobile Cloud Computing (MCC), particularly concerning authentication, privacy, and trust. It identifies shortcomings in existing MCC models, especially regarding cloud-to-client authentication. Despite numerous studies on MCC, security concerns remain inadequately addressed, posing risks to data security, privacy, and integrity. The findings underscore the necessity for comprehensive MCC models that address all security threats, including authentication challenges, to ensure robust protection of data and communication channels. Future research should prioritize developing holistic MCC models that integrate advanced authentication mechanisms and privacy-preserving techniques. Industry stakeholders must prioritize security in MCC implementations to mitigate potential threats and safeguard user privacy and data integrity effectively.

Similarly, Papaioannou et al. [25] keystroke-based authentication is incorporated as a means to enhance security during human-mobile interactions. This authentication method captures the unique typing patterns of smartphone users, adding a layer of security. By analyzing keystroke dynamics, such as typing speed and rhythm, the system can verify the identity of the user. The dataset includes data from various sensors, including the accelerometer, gyroscope, and microphone, to gather comprehensive information about user interactions. Keystroke-based authentication offers a seamless and non-intrusive way to verify user identity while ensuring usability and convenience. This approach contributes to the development of secure authentication mechanisms for mobile devices used in border control scenarios.

Furthermore, the authors analyze several possible authentication attacks, including eavesdropping, Man-in-the-Middle (MITM), replay attacks, session hijacking, Verifier impersonation, and non-repudiation. These attacks pose significant threats to the security of cloud-based systems and can lead to unauthorized access, data breaches, and identity theft. To mitigate these risks, the authors of this study proposed prevention mechanisms outlined in Table 1. These prevention mechanisms likely include a combination of encryption protocols [12], authentication methods, access control measures, and intrusion detection systems [7] designed to detect and thwart potential attacks in cloud environments. Implementing these prevention mechanisms is crucial for safeguarding sensitive data and ensuring the integrity and security of cloud-based services.

Table 1: Possible attacks on Authentication mechanisms

Ref.	Attack	Definition	Prevention Mechanism
[3][10][12] [24][22] [26]	Eavesdropping	Unauthorized persons gain access to an authenticated channel and breach confidentiality	Encryption
[2][26]	MITM	Attacker acts as a sender for the receiver & vice versa	Mutual authentication
[2][26]	Replay	Valid transmission maliciously delayed or repeated	Session tokens
[12]	Session hijacking	Unauthenticated channel, impersonating sender/receiver	Encryption, SSL
[2][23]	Verifier impersonation	Unauthorized user acts as a legitimate user	Challenge response mechanism
[1]	Non-repudiation	Authorized authorities are denying that they are not authenticated	Digital Signature

Analysis of Authentication Mechanisms in MCC: In this section, we have systematically mapped out various authentication schemes discussed in the literature survey according to the evaluation criteria set by the National Institute of Standards and Technology (NIST) [27][28][29][30][31]. In our analysis, we have thoroughly examined a diverse range of authentication techniques employed between mobile terminals and cloud service providers, leveraging the framework provided by the National Institute of Standards and Technology (NIST). This evaluation has enabled us to identify the NIST levels at which these authentication mechanisms operate within the Mobile Cloud Computing (MCC) paradigm. NIST (National Institute of Science and Technology) is a non-regulatory federal agency of the U.S. that plays a crucial role in addressing issues of science and technology.

We have evaluated different authentication mechanisms in the domain of MCC as shown in Table 2, based on the levels of NIST [29]. The protocols meeting the requirements of level 1 include challenge-response protocol and SSO. Simple password challenge-response protocol is evaluated at this level and it combines a password with a challenge to generate an authentication reply. Kerberos, a single sign-on authentication system, validates the principal identities by generating tickets for each service requested by the client. Each ticket has different components: server, client, address, timestamp, lifetime, key (CIS), and key(s). The verifier may obtain a subscriber password from the Cloud Service Provider (CSP) and authenticate the claimant using the challenge-response protocol. This level of authentication aims to prevent replay and online guessing attacks effectively.

In our evaluation, we have determined that single-factor authentication and the Kerberos protocol meet the requirements of level 2 according to the NIST framework. CSP provides a secure mechanism that enables the verifiers to validate the credentials provided by claimants. The verifier authenticates the claimant using a password through a secure encrypted channel, often established through tunneling. This channel effectively safeguards against replay attacks, one-line guessing, and eavesdropping but it remains vulnerable to man-in-the-middle attacks.

The protocols that meet the requirement at level 3 include multi-factor authentication and a one-time password system, bolstered by cryptographic techniques, and meet the stipulated requirements. The cryptographic token is a physical hardware device designed to enhance security in authentication processes. The cryptographic token is used to combine the nonce with a cryptographic key to produce an output that is sent to the verifier as a password. This password is cryptographically generated once. Level 4 provides the highest level of authentication as well as assurance in the practical remote network.

Table 2: Authentication mechanisms

Ref	Authentication Mechanism	Description	Level	Security Features	Security Challenges
[1]	SSO	Username & password, The user logs in once and gains access to all systems	1	Authentication, Authorization	Management of authorized access privilege
[27]	Multi-Level Security Attribute-Based Authentication	This model integrates Attribute-Based Access Control (ABAC) and Attribute-Based Encryption (ABE)	3	Confidentiality + Access control	Its reliance on a specific cryptographic primitive
[2]	MDA	User ID + password +hashing, encrypted hashed message (i.e., message digest) is employed by MDA	3	Confidentiality+ Integrity+ Authentication	Vulnerable to collision attack when two (or more) inputs such that MD5(Message Digest Algorithm 5) will generate the same

					output from different inputs
[2] [32]	Fingerprint	Using the camera of the device	3	Authentication, Authorization	Fake fingerprints
[1] [2]	Multi-factor Authentication	ID/password, voice, and face recognition	3	Authentication	Performance
[28]	quantum key distribution (QKD)	Quantum-based secure communication method	3	Confidentiality + Authentication	Developing robust protocols for secure communication

The authentication techniques are mentioned below in Table 2 along with a description, NIST level, security features, and security challenges. Each authentication technique was analyzed based on its cryptographic functions, which align with the levels defined by the National Institute of Standards and Technology (NIST). Later, in security features, we analyzed the confidentiality, integrity, availability, authentication, and non-repudiation parameters that are covered by different authentication mechanisms. Each authentication mechanisms have different levels from Level 4 to Level 1 and we have analyzed them based on different attacks that have been launched in this mechanism.

Authentication Levels of NIST:

The FIPS 140 Publication Series, issued by NIST, serves as a comprehensive guideline for establishing requirements and standards concerning both hardware and software cryptographic modules [29]. Within this series, FIPS 140-2 delineates four distinct levels of security, denoted from "Level 1" to "Level 4". At Level 1, there exists minimal assurance in asserted identity, where identity proofing may be optional, particularly in cases prioritizing user anonymity. While plaintext passwords cannot be shared over a network, a basic password challenge-response protocol suffices. However, this level remains vulnerable to eavesdropping attacks due to the lack of encryption [29]. Moving up to Level 2, a significantly enhanced security mechanism is implemented, incorporating cryptographic functions for encryption to safeguard against eavesdropping attacks. Additionally, a long-term shared authentication feature is exclusively disclosed to the subscriber and the Cloud Service Provider (CSP). Level 3 introduces a multi-factor remote authentication mechanism, offering users the flexibility to utilize biometric functions or passwords to activate the key and gain system access. Authentication hinges on providing proof of possession of a key or password using a cryptographic protocol. Finally, Level 4, tailored for transactions necessitating the highest confidence in asserted identity accuracy, shares security features with Level 3. Moreover, Level 4 integrates a "hardware cryptographic module" stored within hardware devices. Authentication mandates the claimant to validate control over the token through a secure authentication protocol. Strong cryptographic functions are mandated for all sensitive data transfers, although symmetric key technology may also be employed [29]. The available authentication frameworks focus on different aspects of security, there is always room for improvement. According to NIST evaluation criteria, the level 3 and level 4 authentication mechanisms are considered better approaches for authentication as compared to level 1 and level 2. However, achieving a balance between security and performance remains a challenge, as there is no single technique that fully addresses both aspects without compromising the other. Moreover, resource limitations hinder the implementation of security algorithms used in cloud computing on mobile devices. There is a need for a lightweight secure framework that provides security with minimum communication and processing overhead for mobile devices. Machine learning plays an active role in different fields of life and the integration of machine learning algorithms holds promising results to enhance authentication methods across various fields [4][7][33][30][31][34][35][21][36][37][38][39][40][41][42][43][44][45][46][47][48][48][49][50][51] [52][53].

Navigating Security and Privacy Challenges in MCC:

The integration of emerging technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) presents both promising prospects and formidable challenges concerning security and privacy within the realm of MCC [7][33]. IoT devices, renowned for their pervasive connectivity and data aggregation capabilities, significantly augment the data flow to and processing within the cloud, thereby eliciting apprehensions regarding the confidentiality and integrity of data [12][8][16][6][17][18]. Furthermore, the deployment of AI-driven analytics systems in MCC environments may inadvertently expose sensitive information to potential breaches or unauthorized access. As these technologies advance and become more ubiquitous within MCC ecosystems, proactive measures are imperative to mitigate security vulnerabilities and uphold user privacy. Additionally, while MCC has garnered attention as a cost-effective solution for entrepreneurs and businesses, leveraging third-party services for mobile applications, it concurrently poses significant challenges and threats due to the relinquishment of data control to external entities.

Tabrizchi et al. [1] discussed that MCC networks leverage cloud resources to enhance mobile device capabilities, yet the integration of cloud and mobile introduces security risks due to data transmission over potentially insecure networks. MCC networks and robust authentication mechanisms play a significant role in triggering non-repudiation. By ensuring that users are accurately identified and their actions are securely authenticated, MCC systems can establish a strong foundation for non-repudiation. When users access cloud resources through MCC networks, Multi-Factor Authentication (MFA) and other security measures ensure the identity of the user performing actions [16]. This authentication process generates digital signatures or other forms of cryptographic evidence that tie specific actions to authenticated users. Consequently, in the event of disputes or claims, these digital signatures serve as irrefutable proof of user actions, preventing users from denying their involvement and enhancing non-repudiation in MCC environments.

The general challenges encountered by MCC encompass the establishment of a mobile cloud architecture compatible with heterogeneous wireless networks. Unlike traditional setups, there is no single access platform accommodating all operating systems of mobile devices, and connectivity cannot be guaranteed across all devices. Most people use mobile devices for calls and internet access, and the open accessibility of resources during internet usage exposes users to various threats [3]. However, multiple users who are unaware of the challenges, fail to adequately protect their mobile devices and often store sensitive credentials on their mobile phones without considering potential theft.

In MCC, data accessibility extends beyond the confines of home and office, allowing users to easily access and manage data from anywhere via the cloud. This transition essentially transforms data storage from static locations to a mobile, pocket-sized format. Although prospects of MCC are promising, however, certain threats and limitations persist, including poor connectivity with the internet, bandwidth capacity, mobility management issues [11], and storage space in the mobile device [6][19]. These issues can be resolved by customizing service software deployed on a nearby cloudlet, which are small instance of the cloud. Cloud and mobile device resources should be balanced so they can easily communicate with each other. It is imperative to maintain a balance between cloud and mobile device resources to ensure seamless communication and functionality.

In the domain of MCC, several threats persist including consistency, limited scalability, and portability, primarily due to insufficient security measures and the absence of open standards. The aforementioned threats hinder the rapid expansion of MCC subscribers. The higher authority members of an organization including IT executives and CEOs, express reluctance to adopt cloud services due to concerns regarding security risks, trust issues, and privacy considerations. Cloud service providers have to mark all the security issues to provide a completely secure environment to attract potential customers. Moreover, many areas within MCC, such as intrusion detection and prevention systems, and security and privacy of user's data stored on the cloud server, require further attention and development [12].

Mobile and cloud computing encounter emerging challenges related to confidentiality [20], integrity, authentication, and many of which are rooted in the baseline of virtualization technologies. The use of third-party services in MCC introduces risks related to loss of control over physical infrastructure and shared resource vulnerabilities, impacting security and privacy. Trust in providers' ability to isolate virtual machines and implement robust security measures is crucial to mitigate breaches and uphold data integrity in MCC environments. While, utilizing third-party services, users lack the control over physical hardware infrastructure of the cloud, leading to security threats arising from multiple virtual machines coexisting on a particular physical machine. Trust in cloud service providers is crucial, particularly regarding their ability to properly isolate virtual machines [7]. Since MCC is built upon the cloud computing infrastructure, it inherits and must address challenges faced by cloud computing.

Similarly, many threats are related to identity management and credential theft that lead to security problems [33]. Managing identities and controlling access is a challenging task for cloud providers, particularly as they remotely validate the identity of the user. This challenge is exacerbated when mobile phones are stolen or accessed by unauthorized individuals, and credentials or passwords are stored improperly on the device, leading to potential security breaches.

Practical Implication:

The practical implication of the study on Mobile Cloud Computing (MCC) security is significant for several reasons:

Enhanced Security:

By addressing security vulnerabilities in MCC, the study contributes to enhancing the overall security of mobile cloud environments. This is crucial for ensuring the integrity and confidentiality of data processed and stored in MCC systems.

Improved Authentication Mechanisms:

The study highlights the importance of robust authentication protocols in mitigating security risks in MCC. By analyzing various authentication mechanisms, the study offers insights into effective strategies for enhancing security in mobile cloud environments.

Data Protection:

The innovative solutions proposed in the study aim to safeguard sensitive information in mobile cloud environments. This is essential for protecting user data from unauthorized access and ensuring data privacy.

Cyber Threat Resilience:

The study emphasizes the need for continual research and development efforts to bolster security measures within MCC. This is crucial for ensuring the resilience of mobile cloud environments against evolving cyber threats.

Discussion: The findings of our evaluation indicate that authentication mechanisms in MCC vary in their alignment with NIST levels and their effectiveness in addressing security concerns. Mechanisms such as multi-factor authentication and one-time password systems, which leverage cryptographic techniques, demonstrate greater resilience against a wider range of attacks and are associated with higher NIST levels. However, we observed challenges in achieving a balance between security and performance across different authentication approaches. While some mechanisms excel in providing robust security, they may introduce higher processing overheads or resource requirements, posing challenges for implementation on mobile devices. Additionally, the integration of machine learning holds promise for enhancing authentication methods in MCC, offering opportunities for future research and development in this area. Overall, our analysis underscores the importance of selecting authentication mechanisms that align with the specific security needs and resource constraints of MCC environments, while also highlighting the need for ongoing innovation to address evolving security threats.

Conclusion:

The paper discusses the integration of cloud computing, mobile computing, and wireless networks into the MCC paradigm, highlighting the emergence of new security challenges necessitating more effective security approaches. With the development of the MCC, new security issues have arisen, which require more efficient security approaches. This paper discusses the purpose, the challenges, the architecture, and the standard authentication mechanism of MCC, emphasizing the significance of authentication in accessing web services. Many authentication techniques are discussed in this paper and are thoroughly surveyed. Later, we categorized them based on security features under the NIST evaluation criteria and challenges for helping to identify security solutions for the system. From these techniques, we have concluded that authentication requirements meet the criteria for authentication for mobile devices and mobile users, but security and performance are not addressed on an equal level. Despite fulfilling security needs, performance degradation issues persist. With the help of NIST evaluation criteria, we categorized and analyzed the authentication techniques and identified the possible attacks upon these levels. To enrich the domain of MCC, further research is required to enhance its security.

References:

[1] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, Dec. 2020, doi: 10.1007/S11227-020-03213-1/METRICS.

[2] A. A. Ahmed, K. Wendy, M. N. Kabir, and A. S. Sadiq, “Dynamic Reciprocal Authentication Protocol for Mobile Cloud Computing,” *IEEE Syst. J.*, vol. 15, no. 1, pp. 727–737, Mar. 2021, doi: 10.1109/JSYST.2020.3012986.

[3] A. S. AlAhmad, H. Kahtan, Y. I. Alzoubi, O. Ali, and A. Jaradat, “Mobile cloud computing models security issues: A systematic review,” *J. Netw. Comput. Appl.*, vol. 190, p. 103152, Sep. 2021, doi: 10.1016/J.JNCA.2021.103152.

[4] A. A. Ikram, A. R. Javed, M. Rizwan, R. Abid, J. Crichigno, and G. Srivastava, “Mobile Cloud Computing Framework for Securing Data,” *2021 44th Int. Conf. Telecommun. Signal Process. TSP 2021*, pp. 309–315, Jul. 2021, doi: 10.1109/TSP52935.2021.9522673.

[5] H. Ullah Khan, F. Ali, S. Nazir, of Swabi, and P. Correspondence Habib Ullah Khan, “Systematic analysis of software development in cloud computing perceptions,” *J. Softw. Evol. Process*, vol. 36, no. 2, p. e2485, Feb. 2024, doi: 10.1002/SMR.2485.

[6] A. Aliyu *et al.*, “Mobile Cloud Computing: Taxonomy and Challenges,” *J. Comput. Networks Commun.*, vol. 2020, 2020, doi: 10.1155/2020/2547921.

[7] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, “Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues,” *J. Inf. Secur. Appl.*, vol. 55, p. 102582, Dec. 2020, doi: 10.1016/J.JISA.2020.102582.

[8] S. A. Bello *et al.*, “Cloud computing in construction industry: Use cases, benefits and challenges,” *Autom. Constr.*, vol. 122, p. 103441, Feb. 2021, doi: 10.1016/J.AUTCON.2020.103441.

[9] Z. A. Almusaylim and N. Jhanjhi, “Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing,” *Wirel. Pers. Commun.*, vol. 111, no. 1, pp. 541–564, Mar. 2020, doi: 10.1007/S11277-019-06872-3/METRICS.

[10] M. Ibtihal, E. O. Driss, and N. Hassan, "Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJCAC.2017040103*, vol. 7, no. 2, pp. 27–40, Jan. 1AD, doi: 10.4018/IJCAC.2017040103.

[11] L. Pallavi, B. T. Rao, and A. Jagan, "Mobility Management Challenges and Solutions in Mobile Cloud Computing System for Next Generation Networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 3, pp. 177–192, 2020, doi: 10.14569/IJACSA.2020.0110322.

[12] M. Shabbir *et al.*, "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," *IEEE Access*, vol. 9, pp. 8820–8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

[13] D. G. M. Sunil Kumar, B. Siddardha, A. Hitesh Reddy, Ch.V.Sainath Reddy, Abdul Bari Shaik, "APPLYING THE MODULAR ENCRYPTION STANDARD TO MOBILE CLOUD COMPUTING TO IMPROVE THE SAFETY OF HEALTH DATA," *J Pharm Negat Results*, pp. 1911–1917, doi: 10.47750/pnr.2022.13.s08.231.

[14] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment," *J. Exp. Theor. Artif. Intell.*, vol. 36, no. 1, pp. 147–160, Jan. 2024, doi: 10.1080/0952813X.2022.2135611.

[15] L. Shi, J. Liu, V. Fonseca, P. Walker, A. Kalsekar, and M. Pawaskar, "Correlation between adherence rates measured by MEMS and self-reported questionnaires: A meta-analysis," *Health Qual. Life Outcomes*, vol. 8, no. 1, pp. 1–7, Sep. 2010, doi: 10.1186/1477-7525-8-99/FIGURES/2.

[16] B. B. Sathish and P. Venkataram, "A Dynamic Authentication Scheme for Mobile Transactions," *Int. J. Netw. Secur.*, vol. 8, no. 1, pp. 59–74, 2009.

[17] H. Witte, C. Rathgeb, and C. Busch, "Context-aware mobile biometric authentication based on support vector machines," *Proc. - 2013 4th Int. Conf. Emerg. Secur. Technol. EST 2013*, pp. 29–32, 2013, doi: 10.1109/EST.2013.38.

[18] G. Dandachi, B. El Hassan, and A. El Husseini, "A novel identification/verification model using smartphone's sensors and user behavior," *2013 2nd Int. Conf. Adv. Biomed. Eng. ICABME 2013*, pp. 235–238, Oct. 2013, doi: 10.1109/ICABME.2013.6648891.

[19] L. X. Hung *et al.*, "Activity-based security scheme for ubiquitous environments," *Conf. Proc. IEEE Int. Performance, Comput. Commun. Conf.*, pp. 475–481, 2008, doi: 10.1109/PCCC.2008.4745102.

[20] A. Corradi, R. Montanari, and D. Tibaldi, "Context-based access control management in ubiquitous environments," *Proc. - Third IEEE Int. Symp. Netw. Comput. Appl. NCA 2004*, pp. 253–260, 2004, doi: 10.1109/NCA.2004.1347784.

[21] D. J. S. Raj, "Improved Response Time and Energy Management for Mobile Cloud Computing Using Computational Offloading," *J. ISMAC*, vol. 2, no. 1, pp. 38–49, Mar. 2020, doi: 10.36548/JISMAC.2020.1.004.

[22] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues," *Telecommun. Syst. 2019 732*, vol. 73, no. 2, pp. 317–348, Sep. 2019, doi: 10.1007/S11235-019-00612-5.

[23] A. Fregly, J. Harvey, B. S. Kaliski, and S. Sheth, "Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13871 LNCS, pp. 415–441, 2023, doi: 10.1007/978-3-031-30872-7_16/COVER.

[24] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[25] M. Papaioannou, G. Mantas, A. Essop, P. Cox, I. E. Otung, and J. Rodriguez, "Risk-Based Adaptive User Authentication for Mobile Passenger ID Devices for Land/Sea Border Control," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2021-October, 2021, doi: 10.1109/CAMAD52502.2021.9617802.

[26] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST

Cybersecurity Framework via the Gordon–Loeb Model," *J. Cybersecurity*, vol. 6, no. 1, Jan. 2020, doi: 10.1093/CYBSEC/TYAA005.

[27] N. Mouha and C. Celi, "Extending NIST's CAVP testing of cryptographic hash function implementations," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12006 LNCS, pp. 129–145, 2020, doi: 10.1007/978-3-030-40186-3_7/COVER.

[28] S. Boboň, "Analysis of NIST FIPS 140-2 security certificates." 2021.

[29] M. Fagan *et al.*, "IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog," Nov. 2021, doi: 10.6028/NIST.SP.800-213A.

[30] "NIST roadmap toward criteria for threshold schemes for cryptographic primitives." Accessed: Mar. 28, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8214A.pdf

[31] S. F. Aghili, M. Sedaghat, D. Singelée, and M. Gupta, "MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme," *Futur. Gener. Comput. Syst.*, vol. 131, pp. 75–90, Jun. 2022, doi: 10.1016/J.FUTURE.2022.01.003.

[32] M. S. Sheikh, J. Liang, and W. Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey," *Wirel. Commun. Mob. Comput.*, vol. 2020, 2020, doi: 10.1155/2020/5129620.

[33] K. Benzekki, A. El Fergougui, and A. E. B. Elalaoui, "A Context-Aware Authentication System for Mobile Cloud Computing," *Procedia Comput. Sci.*, vol. 127, pp. 379–387, Jan. 2018, doi: 10.1016/J.PROCS.2018.01.135.

[34] S. Abidin, A. Swami, E. Ramirez-Asís, J. Alvarado-Tolentino, R. K. Maurya, and N. Hussain, "Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC)," *Mater. Today Proc.*, vol. 51, pp. 508–514, Jan. 2022, doi: 10.1016/J.MATPR.2021.05.593.

[35] M. J. O. Saarinen, "WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography," *Proc. 2022 IEEE Int. Symp. Hardw. Oriented Secur. Trust. HOST 2022*, pp. 69–72, 2022, doi: 10.1109/HOST54066.2022.9839849.

[36] T. Hai *et al.*, "An archetypal determination of mobile cloud computing for emergency applications using decision tree algorithm," *J. Cloud Comput.*, vol. 12, no. 1, pp. 1–15, Dec. 2023, doi: 10.1186/S13677-023-00449-Z/TABLES/8.

[37] M. A. Arshed, S. Mumtaz, O. Riaz, W. Sharif, and S. Abdullah, "A Deep Learning Framework for Multi Drug Side Effects Prediction with Drug Chemical Substructure," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 1, pp. 19–31, Jan. 2022, Accessed: Feb. 13, 2024. [Online]. Available: https://journal.50sea.com/index.php/IJIST/article/view/140

[38] M. A. Arshed, H. Ghassan, M. Hussain, M. Hassan, A. Kanwal, and R. Fayyaz, "A Light Weight Deep Learning Model for Real World Plant Identification," *2022 2nd Int. Conf. Distrib. Comput. High Perform. Comput. DCHPC 2022*, pp. 40–45, 2022, doi: 10.1109/DCHPC55044.2022.9731841.

[39] A. Shahzad, M. A. Arshed, F. Liaquat, M. Tanveer, M. Hussain, and R. Alamdar, "Pneumonia Classification from Chest X-ray Images Using Pre-Trained Network Architectures," *VAWKUM Trans. Comput. Sci.*, vol. 10, no. 2, pp. 34–44, Dec. 2022, doi: 10.21015/VTCS.V10I2.1271.

[40] M. Mubeen, M. A. Arshed, and H. A. Rehman, "DeepFireNet - A Light-Weight Neural Network for Fire-Smoke Detection," *Commun. Comput. Inf. Sci.*, vol. 1616 CCIS, pp. 171–181, 2022, doi: 10.1007/978-3-031-10525-8_14/COVER.

[41] M. A. Arshed, S. Mumtaz, M. Hussain, R. Alamdar, M. T. Hassan, and M. Tanveer, "DeepFinancial Model for Exchange Rate Impacts Prediction of Political and Financial Statements," *3rd IEEE Int. Conf. Artif. Intell. ICAI 2023*, pp. 13–19, 2023, doi: 10.1109/ICAI58407.2023.10136658.

[42] "Tomato Disease Classification using Fine-Tuned Convolutional Neural Network," vol. 4, no. 1, pp. 123–134, 2022.

[43] M. A. Arshed, A. Shahzad, K. Arshad, D. Karim, S. Mumtaz, and M. Tanveer, "Multiclass Brain Tumor Classification from MRI Images using Pre-Trained CNN Model," *VFAST Trans. Softw. Eng.*, vol. 10, no. 4, pp. 22–28, Nov. 2022, doi: 10.21015/VTSE.V10I4.1182.

[44] "Machine Learning with Data Balancing Technique for IoT Attack and Anomalies Detection | International Journal of Innovations in Science & Technology." Accessed: Feb. 07, 2024. [Online]. Available: https://journal.50sea.com/index.php/IJIST/article/view/277

[45] H. A. Arshad, M. Hussain, A. Amin, and M. A. Arshed, "Impact of Artificial Intelligence in COVID-19 Pandemic: A Comprehensive Review," *2022 2nd Int. Conf. Distrib. Comput. High Perform. Comput. DCHPC 2022*, pp. 66–73, 2022, doi: 10.1109/DCHPC55044.2022.9732091.

[46] M. A. Arshed, W. Qureshi, M. Rumaan, M. T. Ubaid, A. Qudoos, and M. U. G. Khan, "Comparison of Machine Learning Classifiers for Breast Cancer Diagnosis," *4th Int. Conf. Innov. Comput. ICIC 2021*, 2021, doi: 10.1109/ICIC53490.2021.9692926.

[47] M. A. Arshed and F. Riaz, "Machine Learning for High Risk Cardiovascular Patient Identification 1," *J. Distrib. Comput. Syst.*, vol. 4, no. 2, pp. 34–39, 2021.

[48] M. Hussain, A. Shahzad, F. Liaquat, M. A. Arshed, S. Mansoor, and Z. Akram, "Performance Analysis of Machine Learning Algorithms for Early Prognosis of Cardiac Vascular Disease," *Tech. J.*, vol. 28, no. 02, pp. 31–41, Jun. 2023, Accessed: Feb. 13, 2024. [Online]. Available: https://tj.uettaxila.edu.pk/index.php/technical-journal/article/view/1778

[49] H. Alasmary and M. Tanveer, "ESCI-AKA: Enabling Secure Communication in an IoT-Enabled Smart Home Environment Using Authenticated Key Agreement Framework," *Math. 2023, Vol. 11, Page 3450*, vol. 11, no. 16, p. 3450, Aug. 2023, doi: 10.3390/MATH11163450.

[50] M. Tanveer, A. U. Khan, M. Ahmad, T. N. Nguyen, and A. A. A. El-Latif, "Resource-Efficient Authenticated Data Sharing Mechanism for Smart Wearable Systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2525–2536, Sep. 2023, doi: 10.1109/TNSE.2022.3203927.

[51] K. Ishaq and S. Fareed, "Mitigation Techniques for Cyber Attacks: A Systematic Mapping Study," Aug. 2023, Accessed: Mar. 28, 2024. [Online]. Available: https://arxiv.org/abs/2308.13587v1

[52] K. Ishaq and F. Khan, "Block Chain in the IoT industry: A Systematic Literature Review," Aug. 2023, Accessed: Mar. 28, 2024. [Online]. Available: https://arxiv.org/abs/2308.13613v1

[53] N. A. Nawaz *et al.*, "A comprehensive review of security threats and solutions for the online social networks industry," *PeerJ Comput. Sci.*, vol. 9, p. e1143, Jan. 2023, doi: 10.7717/PEERJ-CS.1143.