https://africanjournalofbiomedicalresearch.com/index.php/AJBR
Afr. J. Biomed. Res. Vol. 27(6s) (December 2024); 432- 443
Research Article

Security and Privacy Enhancement in Mobile-Cloud Computing throughCloud Broker Trust Management using AES Algorithm

Prof. Parthasarathi Murugesan[1*], Dr. Koppula Srinivas Rao[2]

[1*]Research Scholar, Himalayan University, Itanagar, AP India, Parthasarathi.murugesan@gmail.com
[2]Professor, Himalayan University, Itanagar, AP, India.Ksreenu2k@gmail.com

***Corresponding Author:** Prof. Parthasarathi Murugesan
*Research Scholar, Himalayan University, Itanagar, AP India, Parthasarathi.murugesan@gmail.com

ABSTRACT
The mobile-cloud environment has quickly evolved while creating the need for strong frameworksto establish trust and safety to deal with various security and privacy issues in these systems. To overcome these challenges, this study presents a cloud broker trust management system to improve security and privacy in the mobile-cloud systems. The system evaluates cloud service providers interms of trust metrics of security, performance, and privacy with the help of sophisticated trust evaluation algorithms. The study employed the PRISMA methodology, systematically reviewing literature across popular databases such as Google Scholar, Scopus, ScienceDirect, IEEE Xplore, and Research Gate. A total of 454 studies were identified during database searches, with 60 studiesmeeting the inclusion criteria for the final review. The data analysis process identified four key themes related to privacy concerns, security challenges, trust metrics in cloud broker systems, and the role of cloud brokers in managing security and privacy. The findings of this study demonstrate that integrating trust metrics and encryption protocols can significantly improve trust management, paving the way for secure and private mobile-cloud ecosystems. Future research directions focus on enhancing trust evaluation and encryption techniques.

Keywords: Mobile-cloud computing, cloud broker, trust management, security, privacy.

***Author of Correspondence:** Parthasarathi.murugesan@gmail.com*

Received: 30/11/2024 Accepted: 20/12/2024

DOI: https://doi.org/10.53555/AJBR.v27i6S.6814

1. INTRODUCTION

1.1. Research Background

In the modern-day business practices, the significance of mobile computing has become increasing especially after the growth of Information and Communications Technology (ICT). For the last two decades, technological advancements have been playing a significant role in the economic development of the country and mobile phone users are constantly increasing (Chung et al., 2014). Mobile devices like tablets and smartphones are now being used for almost all purposes in life such as internet browsing, chatting, emailing, entertaining, documents editing or sharing, booking movie tickets, ordering food items, etc., During the year 2015, the number of smartphone and tablet users were approximately 1.5 billion and 640 million, respectively (cited in Mollah et al., 2017). These large numbers indicated that different users have different satisfaction levels regarding mobile computing and their computational requirements.

The mobile cloud computing is a cloud computing

service that is provided through either mobile embedded system environment or mobile phone environment. Mobile computing possesses the capability to integrate it with cloud computing due to the traits of cloud model; for instance, measured services, rapid elasticity, resource pooling, broad network access, and on-demand self- service (Mollah et al., 2012). Additionally, mobile users mostly use cloud computing since it provides services like cloud service. A report by ABI (as cited in Mollah et al., 2017) indicated that the cloud service earned 5.2 billion USD revenue approximately till 2015 due to the increasing number of mobile users employed cloud computing services. The number of users was found to be 240 million, as per this report. Wireless communication technologies help mobile users to make use of cloud services (Fernando et al., 2013; Sharma et al., 2013).

The mobile computing has been utilized for showing, processing, transporting and sharingthe resources and applications through wireless communication that help mobile users utilizing network services, resources, and support the communication between clouds and mobile devices. Nowadays, cloud computing offers various applications for mobile users including cloud-assisted Internet of Things (Cahyani et al., 2017), human-centric mobile cloud (Chen et al., 2015b), gaming(Cai et al., 2015), mobile social networks (Nan et al., 2014), education and learning (Ferzli & Khalife, 2011), mobile commerce systems (Yang et al., 2010), cloud-based next-generation cellular networks (Yin et al., 2015), cloud mobile media (Gao et al., 2015), data sharing (Chen et al., 2015a), cloud storage (Ab Rahman et al., 2017), and application processing (Mao et al., 2017),etc., The technological development in the ICT field such as the introduction and widespread adoption of advanced and future 5G millimetre wave (mmWave) wireless communications, fourth- generation/long term evaluation, Wi-Fi, etc., have made individuals to adopt and use cloud servicessimpler and effective (Wu et al., 2015; Hossain & Hasan, 2015).

Zhong et al. (2012) identified MCC should have six characteristics including regional boundary removing, cost-effective on-demand services, efficient processing of tasks, intelligent load balancing, adequate data accessibility, and penetrating hardware limitations. Despite offering various benefits, MCC have certain challenges and limitations that hinders their progress. Some of the challenges and issues noted are Privacy challenges, trust, security, ensuring Quality of Service (QoS), energy efficiency, application services issues, elasticity, cloud policies for mobile users, context-processing, mobility management, process offloading, heterogeneity, scarcity of channel bandwidth, costs of network access, availability, stability, limited resources of mobile devices (Alizadeh & Hassan, 2013; Liu et al., 2013; Amin et al., 2013). Privacy and security-related issues are highly significant to deal with due to various concerns such as heterogeneous environments, distributed cloud storage and processing, resource-constraint mobile devices, and insecure open air transmission medium (Mollah et al., 2017).

1.2. Problem Statement

The arrival of mobile-cloud computing has changed the way mobile devices access cloud services with a wide range of applications, such as storage and high-performance computing (Saemi et al., 2023). In a mobile cloud computing environment with decentralized mobile users and centralized cloud providers, cloud brokers act as intermediaries to mediate the interaction between mobile users and cloud providers to theoretically allocate resources, broker data, and provide services (Filiopoulou et al., 2024). With the growing need for mobile cloud systems, however, mobile cloud systems have gained even greater risk due to the high transfer of sensitive user data through third-party brokers. Because the cloud broker frameworks lack security protocols, mobile users are vulnerable to data breaches, unauthorized access, and privacy violations (Cinar, 2023). Furthermore, cloud providers are very diverse and confound trust management due to the discrepancies in how they secure and comply. This research aims to solve the problem of trust management and data privacy in mobile-cloud computing systems. The focus will be on creating robust security protocols for cloud brokers to adhere to encryption, authentication, and privacy-preserving requirements during cloud interactions to prevent vulnerable mobile data from being inserted into cloud interactions.

1.3. Research Objectives

The objectives of this study are:

1) To study the importance of privacy concerns and need of critical security faced in mobile-cloud computing environments.
2) To develop a cloud broker trust management system to effectively manage the security and privacy by recommending trustworthy cloud service providers.
3) To propose a cloud broker trust management framework by integrating trust metrics (security, reputation, and privacy), and trust evaluation algorithms.
4) To integrate the security encryption for encoding and decoding trust scores and sensitive data for the cloud broker trust management framework.

1.4. Research Questions

Following are the research questions developed from the research objectives:

1) What is the importance of privacy concerns and need of critical security faced in mobile-cloud computing and cloud broker environments?
2) How the cloud broker trust management system helps to manage the security and privacy towards cloud service providers?
3) How the cloud broker trust management framework enhances the trust metrics (security,

reputation, and privacy), and trust evaluation algorithms?
4) How the integration of encryption for encoding and decoding trust scores and sensitive data helps to increase the security of the cloud broker system?

1.5. Significance of the Study

The current study is significant since it provides advanced solutions related to security and privacy requirements for mobile-cloud computing through cloud broker trust management
framework that integrates encryption techniques, evaluation algorithms, and trust metrics. As morefocus businesses nowadays pays to mobile-cloud services, the current study addresses concerns regarding cloud service providers' credibility and the users' data privacy and security. The study also recommends trustworthy providers and safeguards sensitive information, support both service providers and users, as well as improving trust in mobile-cloud environments. This study's findings also help to inform technological innovations in the future and guide policymakers and industry stakeholders to strengthen the cloud security practices.

1.6. Structure of the Study

The rest of the study is organized as follows. The next chapter outlines the PRISMA methodology and identifies and selects relevant articles on privacy and security in mobile-cloud computing. The third chapter "Findings and Analysis" presents the core findings by analysing the themes extracted from the reviewed articles. The last chapter discusses the themes findings from third chapter, summarizes the key findings, and also proposes potential areas for future research to further advance trust management in mobile-cloud environments.

2. RESEARCH METHODOLOGY

This chapter discusses the research methodology employed for this study. The study conducted a comprehensive literature review on security and privacy enhancement in mobile-cloud computing. For this, the study employed PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, known for ensuring transparent, systematic approach in literature reviews (Belle & Zhao, 2023). There are different stages in PRISMA methodology like identifying articles, including articles based on predetermined criterions. PRISMA methodology helps researchers to review fields that contain diverse and extensive literatures and select only the relevant, high-quality articles to be included in the final study. Each stage in PRISMA methodology i.e., developing search strategy, selecting studies, extracting and synthesising data, all are essential in conducting a reliable, in-depth overview of the existing literature on the subject matter (Elshater & Abusaada, 2022).

2.1. PRISMA Methodology for Literature Review

This study chosen the PRISMA methodology since it provides a rigorous, systematic approach in the literature review process especially on complex areas of subject; in this case, security and privacy enhancement in mobile-cloud computing. In this study, it provides a robust framework, allows to conduct a detailed investigation on studies related to cloud broker trust management and security and privacy enhancement in mobile-cloud environments. Following thisPRISMA methodology, the study offers replicability and transparency, allowing future researchers to conduct studies based on the current study's findings.

2.1.1. Search Strategy

The study developed the search strategy related to trust management, privacy, and security with regards to mobile-cloud computing and identified studies. The popular databases andrepositories used for identifying studies were Google Scholar, Scopus, ScienceDirect, IEEE Xplore, and Research Gate. These sources were helpful to find large number of studies with different settings and contexts related to the study topic. Some of the keywords used to perform search operations were "Mobile-Cloud Computing", "Security", "Privacy", "Cloud Broker Trust Management", "Trust Metrics" and "Trust Evaluation Algorithms". The Boolean operators were also employed in varying combinations to improve the search's precision. Overall, these strategies
assisted researcher in identifying studies according to the objectives developed for this study whilemaintaining the rigor and relevance.

2.1.2. Inclusion and Exclusion Criteria

For defining the search results and ensuring relevancy in the research process, it has been essential for the researcher to develop precise inclusion and exclusion criteria. This means that setting up criteria to decide what studies should be included in the final review process and what should be excluded (Peters et al., 2020). In this study, the inclusion criteria used was identifying studies only related to mobile-cloud computing environments that discusses in the contexts of privacy, security, and trust management. Another inclusion criteria were that studies should be published in the last ten years i.e., from 2014 to 2024 in order to select most-relevant studies due to the fact that computing technologies have been evolving over time. These studies must be present only in English language and full-text should be available. Moreover, the researcher chose only the studies which are reviewed by peers, technical reports, and conference papers. On the other hand, studies that lacks empirical data or addresses security mechanisms in general were excluded. All the studies that do not satisfied the inclusion criteria were also excluded. In these ways, the study compiled a focused and reliable set of literature and improved the relevance of the review process.

2.1.3. Study Selection Process

There are four stages in the PRISMA methodology to select studies such as Identification, Screening, Eligibility, and Inclusion (Zsuzsanna, 2022). The first stage, identification, includes searching databases for relevant studies. In this stage, the current study identified 454 studies. After the removal of duplicates i.e., same studies found in different databases, the number of studies was reduced to 285. The second stage, screening, includes the reviewing of titles and abstracts of the identified studies. While in this stage, studies that did not focused on privacy, security, trust management contexts within mobile-cloud computing were excluded. After the exclusion, the number of studies passing the screening stage were found to be 226. The third stage,eligibility, includes the reviewing of full-text studies to determine its relevancy and were found to only 116 studies were passed through this stage. The remaining 110 studies were excluded for several reasons like those studies are thesis papers, review papers, etc., In the last stage, inclusion, the study found only the 60 studies that provided substantial insights into security, privacy, and trust metrics within mobile-cloud computing contexts were eligible for final review. A frameworkdescribing each stage is demonstrated in below figure (Figure 1).

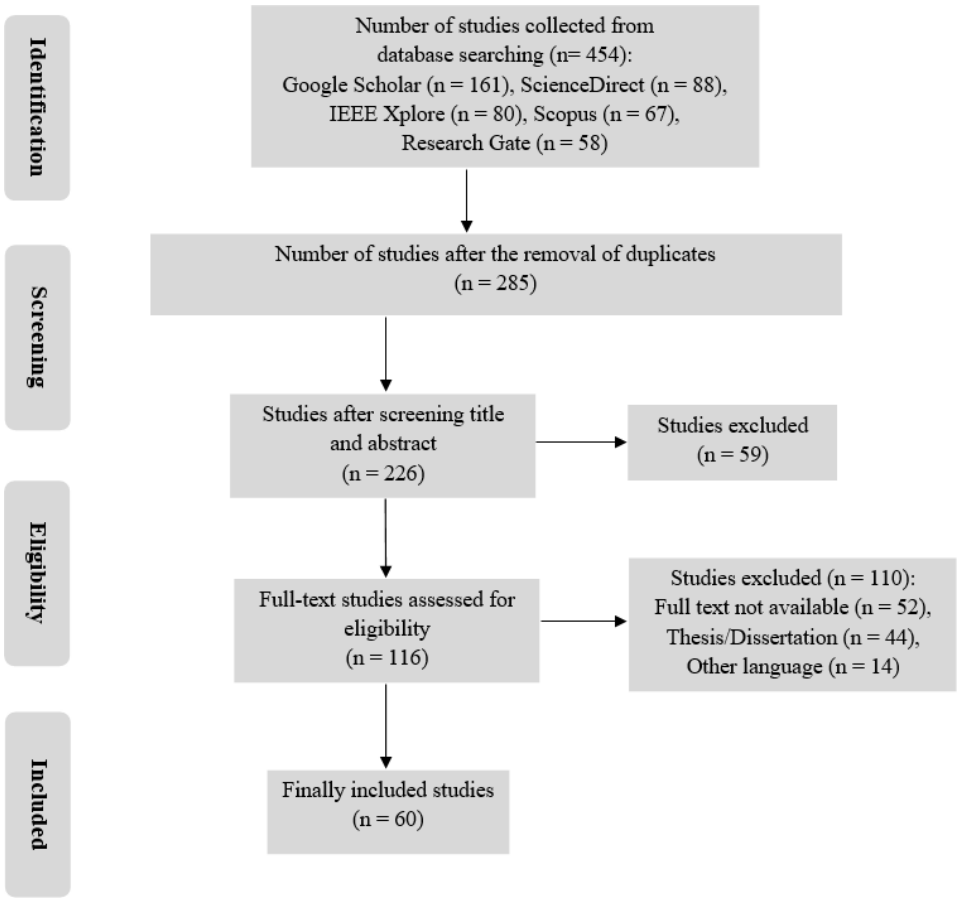

Figure 2.1: PRISMA model

2.1.4. Data Extraction and Synthesis

Data extraction involves systematic classification of important insights such as authorship,publication year, objective(s), methodologies employed, key findings of the study, and limitations in the study. Each study involved in the final review were categorized based on these classifications to help finding themes across studies. A detailed analysis on encryption mechanisms, privacy frameworks, cloud broker trust management practices were obtained by looking at the categorization made in table format. In this study, analyzing themes helped to found recurring themes like the role of encryption in securing trust scores, trust evaluation algorithms, and privacyrisks. Through this extraction and synthesis process, the study also understood the most-relevant methodologies employed by previous studies within the context of trust management and security in mobile-cloud environments, underscoring critical insights and identifying areas for further exploration.

2.1.5. Quality Assessment

Quality assessment has been essential for evaluating the rigor and reliability of each studythat are included for review (Brown et al., 2022). Criterions like generalizability of findings, validity of methodologies used, clarity of the research design are the important indicators of quality assessment. The current study placed emphasis on peer-reviewed studies with strong empirical data; while studies lacking methodological

information or with limited scope were noted but considered cautiously. The quality assessment in this study helped researchers identifying strengths and limitations present in the current literature bodies related to security, privacy, and trust management and also finding areas and gaps to conduct more detailed investigations in futureseeking to address security and privacy in mobile-cloud computing.

2.1.6. Data Analysis

The study used thematic analysis process to analyze data. This process helps the study to organize and synthesize data into four major themes such as privacy concerns in mobile-cloud computing, security challenges in mobile-cloud environments, trust metrics in cloud broker systems, and security and privacy integration in cloud broker trust management. Each theme was explored in detail for identifying unique perspectives, differences, and commonalities related to managing privacy, security, and trust information in mobile-cloud computing contexts. All these themes helped the study to provide an integrated view on privacy, trust, and security information on mobile-cloud computing, providing insights into the best practices and areas for further development.

3. FINDINGS AND ANALYSIS

In this chapter, the key findings are presented and the themes derived from the PRISMA methodology are reviewed. As noted, four major themes emerged in this review study such as privacy concerns, security challenges, trust metrics, and the role of cloud brokers. The below sections discuss each of these themes in detailed and comprehensive manner.

3.1. Privacy Concerns in Mobile-Cloud Computing

Despite mobile-cloud computing offer various benefits to digital business environments, concerns related to privacy always need to be carefully examined. One of the benefits is the combined use of cloud platforms' computational resources and mobile devices' power and convenience (Wang et al., 2015; Botta et al., 2016). In this case, the sensitive personal informationof users may get leaked which questioned the privacy offered by these mobile-cloud applications.

The exposure of risks with regards to cloud infrastructures and mobile devices raises privacy concerns in mobile-cloud ecosystems. Mobile devices can be lost, theft, and used by unauthorized persons owing their portable nature. On the other hand, accessing data and managing control over cloud platforms can be a complicate process since it stores large amount of data across different locations (Almusaylim & Jhanjhi, 2020).

The most notable privacy concern is related to unauthorized access of personal data in mobile-cloud computing environments (Dey et al., 2016). The data sent from mobile devices to the cloud may contain sensitive information like financial details, location data, health records, and personal contact information. In the case of inadequate privacy measures, such information could be leaked and exposed. The encryption mechanisms may not able to stop malicious actors to penetrate through potentially weak cloud channels. Furthermore, mobile applications create vulnerabilities that compromise the privacy of users due to the fact that it sometimes collects personal information without the consent of them (Dey et al., 2016; Alnajrani et al., 2020).

Another concern in the mobile-cloud environment is the lacking of transparency in the data handling practices among cloud service providers. As most of the cloud service providers do not share information related to how user data are stored, processed, and/or shared, the potential risks associated with using these services are not known. Moreover, the increasing size of cloud storagemade users to question how to access and take control over their information through cloud channels. Further to be noted that different countries have their own privacy rights and data protection laws, which complicate the compliance process for cloud providers and create high chance of data being misused (Rustad & Koenig, 2019; Zandesh, 2024).

Various solutions have been proposed in order to mitigate these privacy risks. Personal information can be protected through anonymization of data, developing access control mechanisms and effective encryption schemes (Pratomo et al., 2023). The data can be accessed by authorized users only if they are transferred using end-to-end encryption mechanisms, preventing misuse of information. The privacy can be further improved by using fine-grained access control, which helps individual in specifying who can access their data and under what conditions. Personal identifiable information can be removed while sharing or analysing data through data anonymization techniques, preventing users from identity theft (Murthy et al., 2019; Farayola et al., 2024).

Furthermore, technologies and policies that are developed to preserve privacy can help individuals to have great control and accessibility over their data. For instance, common privacy- enhancing technologies (PETs) including differential privacy, homomorphic encryption, and multi-party computation can greatly help the data analysis process in the cloud environment (Dritsas et al., 2024). It is also the responsibility of cloud providers to ensuring compliance with privacy regulations including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). These regulations create strong data protection measures and allow individuals to have greater control over their data (Daniel & James, 2023).

Addressing privacy concerns of mobile-cloud environments is not without challenges. Firstly, a balance between cloud service functionality and the privacy of users must be achieved (Al-Janabi et al., 2017). For instance, despite encryption mechanisms allow for the protection of sensitive data, the cloud-based services and mobile applications' performance can be negatively impacted by them. Hence, it is the need for achieving balance between maintaining service performance and protecting privacy in order

to create long-term trust among users over mobile-cloud environments. Cloud brokers can positively influence the relationship between cloudproviders and users towards effective mitigation of privacy risks. They also play a significant role in the decision-making processes with regards to the personal data' storage and processing and strategically evaluates cloud service providers and recommends higher standard privacy practices(Abbas, 2023).

Overall, the first theme suggested having a multi-layered approach to address privacy concerns in mobile-cloud computing. This approach should facilitate transparency in the handling of data and integrate regulatory compliance with technological solutions. Continuous assessment and updating privacy measures are also helpful to stay with technological trends and address emerging privacy challenges over time.

3.2. Security Challenges in Mobile-Cloud Environments

Security challenges is another area that need to be considered in mobile-cloud environments. However, various benefits offered by cloud computing technologies and mobile devices such as scalable computing power and ubiquitous access to services (Rahimi et al., 2014), there are some security risks associated with it. Malware infections, physical loss, and theft are some of the common problems that led mobile users prone to different security risks (Ali et al., 2015). Their sensitive personal data in the mobile device can be accessed by attackers especially while transmitting it to the cloud. Denial-of-service attacks, data breaches, and cyberattacks are some common security issues found in the cloud environments while they process the large amountof stored data (Au et al., 2018).

Mobile devices are vulnerable to physical attacks. There is a high chance for a mobile device to lost or stolen due to its portable nature. In this case, attackers get easy access of respective
mobile user's sensitive data such as financial records, emails, and personal contacts (Ismail et al., 2021). In some instances, mobile devices are connected to untrusted and public networks like Wi- Fi hotspots; this can become the primary reason to affect with man-in-the-middle (MITM) attacks. This attack intercepts and manipulates the data that are being transmitted between cloud servers and mobile devices (Mallik, 2019).

Along with these physical risks, malicious and malware applications are another serious security concern need to be considered. Most of the mobile applications, while installing, asks user permissions such as messages, contacts, and location for accessing wide range of their data. In the case of these applications do not have adequate security measures, attackers can easily pass through these systems, penetrate to the mobile devices, access their data unauthorizedly, and have control over the associated cloud systems (Degirmenci, 2020). Malware attacks mean unauthorizedaccessibility to cloud platforms and stealing user data. For instance, botnets deployment could leadto launch various severe malware attacks on cloud infrastructures (Hoque et al., 2015; Karim et al., 2015).

Handling how to store data, process it, and access control is another concern associated with cloud infrastructures as they contain large amount of data. These data are stored in multiple server locations; and hence accessing and securing all data points is a challenging process (Singh& Chatterjee, 2017). Here, breaching of user data is a serious concern that require careful consideration as attackers try to attack cloud providers and get accessibility to sensitive information stored in these servers. Authentication protocol, access control, and encryption mechanisms are commonly used by cloud providers to prevent them from these attacks (Indu et al., 2018). Role-based access control and multi-factor authentication are commonly used nowadays to ensure unauthorized individuals cannot access the data and services provided in the cloud environments. Encryption mechanisms help cloud data from being readable even if it prone to attacks like unauthorized access or data theft (Pookandy, 2021).

Distributed denial-of-service (DDoS) is another attack that challenges the security concern offered by the cloud services. DDoS creates increased illegal traffic to cloud servers that may affectcloud services from being offered to right users (Osanaiye et al., 2016). Load balancing and traffic filtering are some common mitigation strategies that must be employed by cloud providers to deal with these attacks or reduce their impacts in the server (Somani et al., 2017). Moreover, a strong identity and access management (IAM) framework is needed for cloud servers that allow for the authentication of cloud applications and users before it gets used (Olabanji et al., 2024).

Ensuring secure communication between cloud services and mobile devices must be the top-priority to follow in the mobile-cloud environments in order to deal with various security risks. For instance, the Transport Layer Security (TLS) and the Secure Socket Layer (SSL) protocols help data to be efficiently encrypted and share over the internet without losing control (Dastres & Soori, 2020). This encrypted data can be transmitted between cloud servers and mobile devices without getting attacks like tampering with the information in transit or eavesdropping on. These encryption mechanisms solely cannot guarantee security to cloud data. Additional security measures like intrusion detection systems (IDS) need to be incorporated with the encryption mechanisms for monitoring the traffic in the network and detecting potential security breaches (Birkinshaw et al., 2019).

Overall, a comprehensive approach is needed for mobile-cloud environments that implements security practices, policies, and technologies simultaneously across both cloud platforms and mobile devices. Cloud brokers are an important asset in this approach who are responsible at evaluating the security standards and cloud service providers and

provide high- quality security recommendations. They can effectively mitigate the associated security risks and improve the overall security of mobile-cloud ecosystems by ensuring that users choose authenticated cloud providers.

3.3. Trust Metrics in Cloud Broker Systems

Ensuring trust with regards to privacy and security of mobile-cloud computing has been essential in computing technologies. It is the responsibility of cloud brokers to effectively evaluate and recommend trustworthy cloud management practices. Trust metrics have been an important asset in these systems that helps ensuring reputation, privacy, security, and reliability of cloud service providers. These metrics are multifaceted in nature with multiple factors such as performance, reputation, privacy, and security metrics involved within it. Making informed decisions and possessing effective and reliable trust management framework while choosing trustworthy and secured cloud services remain the primary concern for cloud broker systems (Bhushan & Gupta, 2017).

3.3.1. Security Metrics

Security is one among the most vital trust metrics in cloud broker systems. In the data exchanging process or in the context of data being accessed or transferred from cloud to mobile, users want to be sure that this information is secured against any form of intrusion, theft or tampering (Bhatia & Verma, 2017). There are various factors that can help to evaluate the securityof cloud providers such as encryption, authentication, logs and responses to various information security events (Ab Rahman & Choo, 2015). Encryption in the cloud can be a good warning of how safe the cloud provider is; for instance, AES 256 for data that is not in use, SSL/TLS for data
in transit (Schwenk, 2022). In addition, cloud brokers are capable of comparing the current securitystandards and certifications implemented by a given provider for cloud service which may include PCI DSS, SOC 2, ISO/IEC 27001, among others (Sun et al., 2022). The experiences of a cloud provider with security in the past forms another consideration. For instance, the cloud providers who often face instances of hacking or have not been sensitive enough to secure the users' data should be considered untrustworthy. On the other hand, the providers who have put a lot of effort to increase security measures and have not often faced data leakage can be trusted. This information is usually compiled from security audit, security reports, and security assessment studies in order to ascertain whether the cloud services satisfy the security needs of the service consumer (Ismail & Islam, 2020).

3.3.2. Privacy Metrics

Privacy concerns are another vital element to consider within the context of a cloud service provider. The privacy metric measures how users' data is in the cloud services offered by the provider. This metric may contain information on where the data is stored, and the provider's policies concerning data ownership (Domingo-Ferrer et al., 2019). Also, some privacy metrics may cover matters to do with data access, third-party data sharing, or the availability of clear data collection policies by the provider. Privacy-memory technologies, which include differential privacy, data anonymization, can also serve as evaluating components of privacy metrics (Janghyun et al., 2022). However, to give a broad measure of privacy, the privacy metric may incorporate privacy standards of the particular cloud provider relative to international privacy such as the ones permitted in Europe in form of the GDPR, or privacy laws as embodied by the CCPA and other regional practices. These regulations put strict guidelines on how the user data must be processed and therefore provides users with more confidence (Bakare et al., 2024).

3.3.3. Performance Metrics

Another important trust metric in cloud broker systems is the performance where reliability of the service is affecting the user's experience in mobile-cloud computing environments (Laghari et al., 2024). This metric evaluates the effectiveness of a cloud provider in the manner that the services are delivered with availability, uptime, and speed. For instance, a provider that offers a very high availability of 99.99 per cent uptime and quick response time will definitely be trusted by users. Cloud brokers compare certain key contractual metrics, the provider's previous uptimes, and other vital performance statistics. Scalability may also be observed as a criterion in performance metrics. As much as resources could be scaled to meet demand, a cloud service provider with limited scalability capability is most often distrusted. This must guarantee that the users have confidence in the cloud provider to meet burst time or any time when the demand for resources is high without compromising on the services to be delivered (Noor et al., 2018; Aslanpour et al., 2020).

3.3.4. Trust Evaluation Algorithms

After identifying and measuring trust metrics, the next step is their incorporation into the trust evaluation models. These algorithms use different metrics to provide overall level of trust for the cloud service provider (Damera et al., 2020). The key challenge found in this trust evaluation algorithm design is the dependence of the optimization of weights for the various trust metrics. For instance, in security-sensitive applications, security may be preferred over performance; while in applications that involve sensitive data, privacy may be preferred over other parameters. Other trust assessment algorithms employ a variety of metrics, which are then integrated using measures from the Bayesian networks, machine learning, or weighted sum models (Wang et al., 2020;
Alhandi et al., 2023). Cloud brokers employ these algorithms to evaluate and compare the level of trust with the possible cloud providers. It will then help them identify the most credible service providers for

users depending on their preference and needs. This aids users in making informed decisions in securing as well as in maintaining privacy in a mobile-cloud computing setting (Singh& Sidhu, 2017).

3.4. Role of Cloud Brokers in Managing Security and Privacy

As sensitive data of users are stored in the cloud platforms, ensuring privacy and security is important for cloud brokers in mobile-cloud computing environments. Cloud brokers should assess the privacy and security measures of these providers and also ensure that both the data and the trust evaluation scores are well-protected (Abdić, 2024). The below sections explore how security and privacy measures are integrated within the cloud broker systems, and identifying their role towards improving the overall reliability and trustworthiness of cloud service providers.

3.4.1. Encryption for Trust Management

The trust evaluation scores and the data managed by cloud brokers are protected by the means of encryption (Seth et al., 2022). It is therefore important to ensure that the metrics used to create trust remain complete and private during the process of evaluating trust in order to avoid compromise. Encryption algorithms such as Transport Layer Security (TLS) or SSL for data in transit and AES-256 for data encryption. Through these algorithms, both user's sensitive information and trust evaluation data are secure till the end (Dechand et al., 2019). Cloud brokers apply encryption for keeping trust assessment criteria, which is used in evaluation of reliability and security of cloud service providers. For example, when the trust scores are produced using results of performance, privacy, and security of a particular site or its user, these scores should
then be encoded and secured especially when passed onto the users. If the scores are not encrypted, they could be intercepted, modified, disclosed to the wrong parties, which would compromise the cloud broker's trust management system. Thus, incorporation of encryption protocol within the cloud broker system is not only obligatory from the security perspective but also necessary to maintain the credibility of the cloud ecosystem (Tang et al., 2016; Kumar & Goyal, 2022).

3.4.2. Privacy-Preserving Technologies

Another factor that is critical to embedding privacy and security is the interoperation of privacy-preserving technologies inside the cloud broker systems (Sun, 2019). Cloud brokers should make sure that the cloud service providers that they recommend meet privacy policies of user data, and the guidelines on internet privacy like the CCPA and GDPR (Bakare et al., 2024). Privacy enhancing technologies are intended to enhance identity privacy and prevent data unauthorized access. For instance, in personal data operation, there are operations that must be conducted by the cloud service provider while the identity of the users and their personalinformation must be protected; such operations can be done using data anonymization. Another such technique that cloud providers can use to gain insights from the massive amounts of data collected is differential privacy. Through these techniques, cloud service providers can offer higherprivacy standards yet they can be capable in transforming ad utilize data as well as delivering services effectively (Kumar & Goyal, 2019; Cinar, 2023). Also, when a cloud broker has the responsibility to determine and control the trust scores, they have to guarantee that these scores are produced and disseminated without any influence to the privacy of the related actors. This can be done using privacy-preserving measures like Secure Multi-Party Computation (SMPC), which enables data to be processed in such a manner that no two parties having the full data set can have sight of the other's data at any one time. It may help, for example, when brokers try to evaluate
the reliability of multiple cloud providers and their honesty without disclosing their clients' data. Privacy preserving technologies not only assist in protecting sensitive data but also guarantee to cloud brokers that they are compliant with merged international privacy regulations (Akremi & Rouached, 2021; Dritsas et al., 2024). As users become more conscious of their privacy, they are more inclined to go for those cloud service providers who incorporate their privacy rights into considerations; thus, it becomes almost indispensable that privacy-enhancing technologies form part of the trust management framework.

3.4.3. Compliance with Regulations

As for cloud brokers, compliance with regulations of privacy and security is one of the most vital prerequisites for gaining mobile-cloud business acceptance. There is also increased concern on privacy and this has given rise to very strict policies like the CCPA and GDPR (Bakare et al., 2024). These regulations demonstrate how data should be processed by cloud providers. For this reason, cloud brokering plays the role of a mediator, and they must meet these well-structured regulations to avoid legal consequences of handling user data. Regulatory conformity can be measured by the analysis of governance certification and standards maintained by cloud service providers alongside an evaluation of the auditing processes followed by cloud service providers. For example, for the providers with the ISO/IEC 27001 certifications, it indicates that they have set the privacy and security elements to the highest level (Mesquida & Mas, 2015). Moreover, those cloud providers that meet to the standard proposed by the GDPR – the right to erasure, minimization of data, and permission – will attract users who are concerned with issues of privacy. As for these regulatory requirements, cloud brokers are to incorporate them into their trust management so that only services with the highest security and privacy standards would be offered. This may require the frequent monitoring of the cloud service providers, checking on the policies

they have put in place regarding the privacy of data, and checking on how these service providers handle data with the aim of making sure that they are fully compliant with the existing legal requirements. Lack of compliance with regulatory requirements may lead to negative consequences such as reputation loss for both the cloud broker and the cloud service provider, as well as legal ramifications for mishandling user data (Singh et al., 2024). Integrating compliance requirements into the management of trust not only offers legal guidance to cloud brokers and users but also enhances the trust in the cloud computing context. To promote a better and safer mobile-cloud environment, cloud brokers make recommendations on cloud providers that meet the necessary security and privacy laws (Marimuthu et al., 2022; Collier, 2023).

4. DISCUSSION AND CONCLUSION

In this chapter, the themes identified in the previous chapter are discussed. It has been understood that these themes are helpful in understanding how privacy and security can be enhanced in mobile-cloud computing environments. The role of cloud broker trust management system was also identified as an important component that ensures the trustworthiness of cloud services.

The first theme, "Privacy concerns in mobile-cloud computing" discussed what are all the privacy risks present in the connection between mobile devices and cloud services. Unauthorizedaccess and data breaches issues were the significant concerns noted and how anonymization and data encryption measures help to control these privacy-related risks. The sensitive information of users has been protected through implementing these measures in real-time cloud environment andensure privacy is not compromised in the overall network. The second theme, "Security Challengesin Mobile-Cloud Environments" discussed the primary security threats including unencrypted data transfer, malware attacks, and data breaches in the mobile-cloud computing environments. This theme also recognized the need for multi-layered defense strategies and strong security protocols to be implemented in the cloud broker frameworks to deal with different security challenges. Handling such security related issues can ensure the trust management system to be resilient that mobile users can depend on. The third theme, "Trust Metrics in Cloud Broker Systems" exploredhow important some trust metrics are (privacy, security, performance) in evaluating cloud serviceproviders. Cloud brokers may use these metrics in assessing the reliability of cloud service providers and integrating it with the needs of users for private and secure cloud services. These metrics also deliver trustworthy and accurate recommendations for cloud services. The final theme, "Role of Cloud Brokers in Managing Security and Privacy" discussed the intermediary role of cloud brokers in the mobile-cloud environment that helps to build improved trust between cloudservices and mobile devices. They evaluate and recommend cloud service providers with improved privacy and security standards and adds value to the overall services offered. They also offer trustworthy, reliable data handling processes.

Overall, the study offered insights on how important is to build trust management and the role of cloud brokers in it towards improving cloud services' privacy and security. Cloud brokers make use of regulatory compliance measures, privacy-enhancing technologies, and different trust metrics to provide reliable and trustworthy recommendations for cloud service providers. Moreover, the trust scores' integrity can be improved through integrating blockchain technologies or encryption mechanisms. The study also found out that cloud brokers play a significant role in the relationship between cloud service providers and mobile users. In particular, the mobile-cloud environment becomes trustworthy if cloud brokers pay more attention to trust scores' integrity, privacy, and security. This not only builds confidence among users but also ensures that data is protected at all stages of the cloud service interaction. Future research should focus on refining trust evaluation algorithms, exploring the role of artificial intelligence in predicting trustworthiness, and developing advanced privacy-preserving technologies within the mobile- cloud environments. Further studies could also investigate the scalability of blockchain for trust score management in large-scale cloud broker systems.

REFERENCES

1. Ab Rahman, N. H., & Choo, K. K. R. (2015). A survey of information security incident handlingin the cloud. computers & security, 49, 45-69.
2. Ab Rahman, N. H., Cahyani, N. D. W., & Choo, K. K. R. (2017). Cloud incident handling and forensic-by-design: cloud storage as a case study. Concurrency and Computation: Practice and Experience, 29(14), e3868.
3. Abbas, A. (2023). Cloud Access Security Brokers (CASBs): Enhancing Cloud Security Posture.
4. Abdić, A. (2024). Enhancing Security and Privacy in Cloud Networking: An In-depth Analysis of Current Techniques, Challenges, and Best Practices. Innovative Computer Sciences Journal, 10(1), 1-6.
5. Akremi, A., & Rouached, M. (2021). A comprehensive and holistic knowledge model for cloud privacy protection. The Journal of Supercomputing, 1-33.
6. Alhandi, S. A., Kamaludin, H., & Alduais, N. A. M. (2023). Trust evaluation model in IoT environment: a comprehensive survey. Ieee Access, 11, 11165-11182.
7. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383.
8. Alizadeh, M., & Hassan, W. H. (2013). Challenges and opportunities of mobile cloud computing. In 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 660-666). ieee.

9. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Abdelhag, M. (2017). Mobile cloud computing: challenges and future research directions. In 2017 10th international conference on developments in esystems engineering (DeSE) (pp. 62-67). IEEE.
10. Almusaylim, A. Z., & Jhanjhi, N. Z. (2020). Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. Wireless Personal Communications, 111(1), 541-564.
11. Alnajrani, H. M., Norman, A. A., & Ahmed, B. H. (2020). Privacy and data protection in mobile cloud computing: A systematic mapping study. Plos one, 15(6), e0234312.
12. Amin, M. A., Bakar, K. B. A., & Al-Hashimi, H. (2013). A review of mobile cloud computing architecture and challenges to enterprise users. In 2013 7th IEEE GCC Conference and Exhibition (GCC) (pp. 240-244). IEEE.
13. Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. Internet of Things, 12, 100273.
14. Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on mobile cloud—Chances and challenges over advanced persistent threat. Future Generation Computer Systems, 79, 337-349.
15. Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. Computer Science & IT Research Journal, 5(3), 528-543.
16. Belle, A. B., & Zhao, Y. (2023). Evidence-based decision-making: On the use of systematicity cases to check the compliance of reviews with reporting guidelines such as PRISMA 2020. Expert Systems with Applications, 217, 119569.
17. Bhatia, T., & Verma, A. K. (2017). Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues. The Journal of Supercomputing, 73, 2558-2631.
18. Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of- art. International Journal of Big Data Intelligence, 4(2), 81-107.
19. Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. Journal of Network and Computer Applications, 136, 71-85.
20. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future generation computer systems, 56, 684-700.
21. Brown, G. T., Bekker, H. L., & Young, A. L. (2022). Quality and efficacy of multidisciplinary team (MDT) quality assessment tools and discussion checklists: a systematic review. BMC cancer, 22(1), 286.
22. Cahyani, N. D. W., Martini, B., Choo, K. K. R., & Al-Azhar, A. M. N. (2017). Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study. Concurrency and Computation: Practice and Experience, 29(14), e3855.
23. Cai, W., Zhou, C., Li, M., Li, X., & Leung, V. C. (2015). Mcg test-bed: An experimental test-bedfor mobile cloud gaming. In Proceedings of the 2nd Workshop on Mobile Gaming (pp. 25-30).
24. Chen, F., Zhang, C., Wang, F., Liu, J., Wang, X., & Liu, Y. (2015a). Cloud-assisted live streaming for crowdsourced multimedia content. IEEE Transactions on Multimedia, 17(9), 1471- 1483.
25. Chen, M., Zhang, Y., Li, Y., Hassan, M. M., & Alamri, A. (2015b). AIWAC: Affective interaction through wearable computing and cloud technology. IEEE Wireless Communications, 22(1), 20-27.
26. Chung, K. Y., Yoo, J., & Kim, K. J. (2014). Recent trends on mobile computing and future networks. Personal and Ubiquitous Computing, 18, 489-491.
27. Cinar, B. (2023). The Role of Cloud Service Brokers: Enhancing Security and Compliance in Multi-cloud Environments. Journal of Engineering Research and Reports, 25(10), 1-11.
28. Collier, B. (2023). Considerations for Selecting and Implementing Cloud Security Solutions Using Cloud Access Security Brokers (Doctoral dissertation, Marymount University).
29. Damera, V. K., Nagesh, A., & Nagaratna, M. (2020). Trust evaluation models for cloud computing. environment, 11, 12.
30. Daniel, B., & James, G. (2023). Cloud Data Privacy: Trends, Challenges, and Future Outlook.
31. Dastres, R., & Soori, M. (2020). Secure socket layer (SSL) in the network and web security. International Journal of Computer and Information Engineering, 14(10), 330- 333.
32. Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 401-415). IEEE.
33. Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261-272.
34. Dey, S., Sampalli, S., & Ye, Q. (2016). Security and privacy issues in mobile cloud computing. International Journal of Business and Cyber Security, 1(1).
35. Domingo-Ferrer, J., Farras, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications, 140, 38-60.
36. Dritsas, E., Trigka, M., & Mylonas, P. (2024). A Survey on Privacy-Enhancing Techniques in the Era of Artificial Intelligence. In Novel &

Intelligent Digital Systems Conferences (pp. 385-392). Cham: Springer Nature Switzerland.
37. Elshater, A., & Abusaada, H. (2022). Developing process for selecting research techniques in urban planning and urban design with a PRISMA-Compliant Review. Social Sciences, 11(10), 471.
38. Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal, 5(3), 606-615.
39. Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future generation computer systems, 29(1), 84-106.
40. Ferzli, R., & Khalife, I. (2011). Mobile cloud computing educational tool for image/video processing algorithms. In 2011 Digital Signal Processing and Signal Processing Education Meeting (DSP/SPE) (pp. 529-533). IEEE.
41. Filiopoulou, E., Chatzithanasis, G., Michalakelis, C., & Nikolaidou, M. (2024). Cloud Broker: Customizing Services for Cloud Market Requirements. Information, 15(4), 232.
42. Gao, G., Zhang, W., Wen, Y., Wang, Z., & Zhu, W. (2015). Towards cost-efficient video transcoding in media cloud: Insights learned from user viewing patterns. IEEE Transactions on Multimedia, 17(8), 1286-1296.
43. Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2242-2270.
44. Hossain, E., & Hasan, M. (2015). 5G cellular: key enabling technologies and research challenges. IEEE Instrumentation & Measurement Magazine, 18(3), 11-21.
45. Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.
46. Ismail, M., El-Rashidy, N., & Moustafa, N. (2021). Mobile cloud database security: problems and solutions. Fusion: Practice and Applications, 7(1), 15-29.
47. Ismail, U. M., & Islam, S. (2020). A unified framework for cloud security transparency and audit. Journal of information security and applications, 54, 102594.
48. Janghyun, K., Barry, H., & Tianzhen, H. (2022). A review of preserving privacy in data collectedfrom buildings with differential privacy. Journal of Building Engineering, 56, 104724.
49. Karim, A., Ali Shah, S. A., Salleh, R. B., Arif, M., Noor, R. M., & Shamshirband, S. (2015). Mobile botnet attacks-an emerging threat: Classification, review and open issues. KSII Transactions on Internet and Information Systems (TIIS), 9(4), 1471-1492.
50. Kumar, R., & Goyal, R. (2019). Assurance of data security and privacy in the cloud: A three-dimensional perspective. Software Quality Professional, 21(2), 7-26.
51. Kumar, R., & Goyal, R. (2022). Performance based Risk driven Trust (PRTrust): On modeling ofsecured service sharing in peer-to-peer federated cloud. Computer Communications, 183, 136-160.
52. Laghari, A. A., Zhang, X., Shaikh, Z. A., Khan, A., Estrela, V. V., & Izadi, S. (2024). A review on quality of experience (QoE) in cloud computing. Journal of Reliable Intelligent Environments, 10(2), 107-121.
53. 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, 20(3), 14-22.
54. Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109-134.
55. Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE communications surveys & tutorials, 19(4), 2322-2358.
56. Marimuthu, M., Akilandeswari, J., Varasree, B., KUMAR, G. R., & Ramasubbareddy, S. (2022). Cloud Broker Recommendation Framework to Provide Trustworthy Cloud Services to the End User: Cloud Broker Recommendation Framework to provide Trustworthy cloud services to the End user. Scalable Computing: Practice and Experience, 23(4), 303-319.
57. Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. Computers & Security, 48, 19-34.
58. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 84, 38-54.
59. Mollah, M. B., Islam, K. R., & Islam, S. S. (2012). Next generation of computing through cloud computing technology. In 2012 25th IEEE Canadian conference on electrical and computer engineering (CCECE) (pp. 1-6). IEEE.
a. Murthy, S., Bakar, A. A., Rahim, F. A., & Ramli, R. (2019). A comparative study of data anonymization techniques. In 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp.306-309). IEEE.
60. Nan, G., Mao, Z., Li, M., Zhang, Y., Gjessing, S., Wang, H., & Guizani, M. (2014). Distributed resource allocation in cloud-based wireless multimedia social networks. IEEE Network, 28(4), 74-80.
61. Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Mobile cloud computing: Challenges and future research directions. Journal of Network and Computer Applications, 115, 70- 85.

62. Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Authorization, and Access Control within Cloud-Based Systems (January 25, 2024).
63. Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications, 67, 147-165.
64. Peters, M. D., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., ... & Khalil, H. (2020). Updated methodological guidance for the conduct of scoping reviews. JBI evidencesynthesis, 18(10), 2119-2126.
65. Pookandy, J. (2021). Multi-factor authentication and identity management in cloud CRM with best practices for strengthening access controls. International Journal of Information Technology & Management Information System (IJITMIS), 12(1), 85-96.
66. Pratomo, A. B., Mokodenseho, S., & Aziz, A. M. (2023). Data encryption and anonymization techniques for enhanced information system security and privacy. West Science Information System and Technology, 1(01), 1-9.
67. Rahimi, M. R., Ren, J., Liu, C. H., Vasilakos, A. V., & Venkatasubramanian, N. (2014). Mobile cloud computing: A survey, state of art and future directions. Mobile Networks andApplications, 19, 133-143.
68. Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. Fla. L. Rev., 71, 365.
69. Saemi, B., Hosseinabadi, A. A. R., Khodadadi, A., Mirkamali, S., & Abraham, A. (2023). Solvingtask scheduling problem in mobile cloud computing using the hybrid multi-objective Harris Hawks optimization algorithm. IEEE Access, 11, 125033-125054.
70. Saravanan, K., & Rajaram, M. (2015). An exploratory study of cloud service level agreements- state of the art review. KSII Transactions on Internet and Information Systems (TIIS), 9(3),843-871.
71. Schwenk, J. (2022). Attacks on SSL and TLS. In Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications (pp. 267-328). Cham: Springer International Publishing.
72. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.
73. Sharma, R., Kumar, S., & Trivedi, M. C. (2013). Mobile cloud computing: Bridging the gap between cloud and mobile devices. In 2013 5th international conference and computational intelligence and communication networks (pp. 553-555). IEEE.
74. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.
75. Singh, M. M. K., Chandna, M., & Kongala, V. Y. Y. (2024). Risk Management Framework for Cloud Migration and Selection of Suitable Cloud Service Provider. Advances in Enterprise Technology Risk Assessment, 283.
76. Singh, S., & Sidhu, J. (2017). Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers. Future Generation Computer Systems, 67, 109-132.
77. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Rajarajan, M., & Buyya, R. (2017). Combating DDoS attacks in the cloud: requirements, trends, and future directions. IEEE Cloud Computing, 4(1), 22-32.
78. Sun, N., Li, C. T., Chan, H., Le, B. D., Islam, M. Z., Zhang, L. Y., ... & Armstrong, W. (2022). Defining security requirements with the common criteria: Applications, adoptions, and challenges. IEEE Access, 10, 44756-44777.
79. Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. Ieee Access, 7, 147420-147452.
80. Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., & Buyya, R. (2016). Ensuring security and privacy preservation for cloud data services. ACM Computing Surveys (CSUR), 49(1), 1-39.
81. Wang, J., Jing, X., Yan, Z., Fu, Y., Pedrycz, W., & Yang, L. T. (2020). A survey on trust evaluation based on machine learning. ACM Computing Surveys (CSUR), 53(5), 1-36.
82. Wang, Y., Chen, I. R., & Wang, D. C. (2015). A survey of mobile cloud computing applications: perspectives and challenges. Wireless Personal Communications, 80, 1607-1623.
83. Wu, D., Wang, J., Cai, Y., & Guizani, M. (2015). Millimeter-wave multimedia communications: challenges, methodology, and applications. IEEE communications Magazine, 53(1), 232- 238.
84. Yang, X., Pan, T., & Shen, J. (2010). On 3G mobile e-commerce platform based on cloud computing. In 2010 3rd IEEE International Conference on Ubi-Media Computing (pp. 198-201). IEEE.