

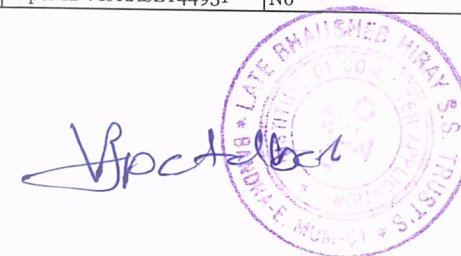
3.3.1 Number of research papers published per teacher in the Journals notified on UGC CARE list during the last five years

Title of paper	Name of the author/s	Department of the	Name of journal	Calendar Year of	ISSN number	Link to the recognition in UGC enlistment of the Journal /Digital Object		
Protecting Data on Mobile Cloud Computing	Vikram Patalbansi	MCA	International Journal of Innovative Technology and Exploring Engineering (IJITEE)	2019	2278-3075	<a href="https://www.ijitee.org/">https://www.ijitee.org/</a>	<a href="https://www.ijitee.org/download/volume-8-issue-11">https://www.ijitee.org/download/volume-8-issue-11</a>	UGC Care and Scopus Listed
Literature Review on Software Reliability and Software Quality Prediction	Sadhana Ojha	MCA	International Journal of Research and Analytical Reviews (IJRAR)	2018	E-ISSN : 2348-1269 P-ISSN: 2349-5138	<a href="http://www.ijrar.org">www.ijrar.org</a>	<a href="http://www.ijrar.org">www.ijrar.org</a> , Volume 6 Issue 1 March 2018	
A Summary of Comparative Study of Software Reliability	Rashmita Pradhan	MCA	International Journal of Research and Analytical Reviews (IJRAR)	2018	E-ISSN : 2348-1269 P-ISSN: 2349-5138	<a href="http://www.ijrar.org">www.ijrar.org</a>	<a href="http://www.ijrar.org">www.ijrar.org</a> , Volume 5 Issue 1 March 2018	
Software Release Policy	Sadhana Ojha	MCA	International Conference 2019 “Convergence of Social Innovation and Digital Transformation in Business” (ICCSIDTB-2019) 5 <sup>th</sup> , 6 <sup>th</sup> April 2019	2019				UGC Care
SURVEY ON SECURITY CHALLENGES AND ITS SOLUTION ON MOBILE CLOUD COMPUTING	Vikram Patalbansi	MCA	Juni Khyat	2020	2278-4632	<a href="https://junikhyatjournal.com">https://junikhyatjournal.com</a>	<a href="https://junikhyatjournal.com/no_1_may_20/27.pdf">https://junikhyatjournal.com/no_1_may_20/27.pdf</a>	UGC Care Listed
Authentication Theory for Mobile Cloud Computing	Vikram Patalbansi	MCA	Journal of Xi'an University of Architecture & Technology	2020	1006-7930	<a href="https://xajzkjdx.cn/volume-xii-issue-10-october-2020/">https://xajzkjdx.cn/volume-xii-issue-10-october-2020/</a>	<a href="https://doi.org/10.37896/JXAT12.10/29593">https://doi.org/10.37896/JXAT12.10/29593</a>	Scopus Listed
Mobile Cloud Computing Cryptographic Scheme	Vikram Patalbansi	MCA	Journal of University of Shanghai for Science and Technology	2021	1007-6735	<a href="https://jusst.org/">https://jusst.org/</a>	<a href="https://jusst.org/archive/">https://jusst.org/archive/</a>	Scopus Listed
Secure Wireless Communication for Mobile Cloud Computing Multimedia Contents	Vikram Patalbansi	MCA	GIS SCIENCE JOURNAL	2021	1869-9391	<a href="https://gisscience.net">https://gisscience.net</a>	<a href="https://gisscience.net/volume-8-issue-4-2021/">https://gisscience.net/volume-8-issue-4-2021/</a>	UGC Care and Scopus Listed

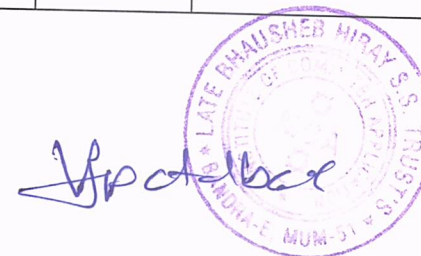


*Handwritten signature in blue ink, likely of Vikram Patalbansi.*

Mobile Cloud Computing Cryptographic Scheme	Vikram Patalbansi	MCA	Journal of University of Shanghai for Science and Technology	2021	1007-6735	<a href="https://jusst.org/Volume%20Issue%206">https://jusst.org/Volume 23 Issue 6</a>	<a href="https://jusst.org/archive/">https://jusst.org/archive/</a>	UGC Care and Scopus Listed
Cloud Storage System for Mobile Cloud Computing using Blockchain	Vikram Patalbansi	MCA	Emerging Trends in Materials, Computing and Communication Technologies 'ICETMCCT 2021' Organized by ANNAI VAILANKANNI COLLEGE OF ENGINEERING, AVK Nagar, Pottalkulam during December 9, 2021 and December 10, 2021	2021		<a href="https://ijsrset.com/paper/vqj8C.pdf">https://ijsrset.com/paper/vqj8C.pdf</a> <a href="https://ijsrset.com/paper/vqj8C.pdf">https://ijsrset.com/paper/vqj8C.pdf</a>	<a href="https://ijsrset.com/paper/vqj8C.pdf">https://ijsrset.com/paper/vqj8C.pdf</a>	
Recognize Candidate Task for Robotics Process Automation	Bhanudas Satam	MCA	International Journal of Research in Applied Science & Engineering Technology	2022	IJRASET45037	<a href="http://www.ijraset.com">www.ijraset.com</a>	<a href="http://www.ijraset.com">www.ijraset.com</a> Volume 10 Issue VI June 2022	
A Study on Reliability of Software Metrics in Software Products	Sadhana Ojha	MCA	Sodhsamhita	2022				UGC Care
A Study on Software Quality and Attributes	Rashmita Pradhan	MCA	Shodhsamhita Volume No. VIII Issue 11 (II) 2021-22	2022	2277-7067		Volume No. VIII Issue 11 (II) 2021-22	UGC Care Listed
Blockchain Difficulties and Valuable Open Doors : A Study	Divakar Jha	MCA	International Journal for Research in Applied Science and Engineering Technology	2022	10.22214	<a href="https://www.ijraset.com">https://www.ijraset.com</a>	Paper ID : IJRASET44931	No



Importance and Application of COBOL in Banking Sectors	Divakar Jha	MCA	International Journal of Advanced Research in Science , Communication and Technology	2022	2581-9429	<a href="https://www.ijarsct.co.in">https://www.ijarsct.co.in</a>	DOI : 10.48175/IJRSCT-5405	
Blockchain-Based Multi-Factor Mobile Device Authentication Technique in Mobile Cloud Computing	Vikram Patalbansi	MCA	Journal of Harbin Engineering University ISSN: 1006-7043	2023	1006-7043	<a href="https://harbinengineeringjournal.com/index.php/journal">https://harbinengineeringjournal.com/index.php/journal</a>	<a href="https://harbinengineeringjournal.com/index.php/journal/article/view/1177">https://harbinengineeringjournal.com/index.php/journal/article/view/1177</a>	Scopus Listed
Packet Cryptography Technique for Data Transit in Mobile Cloud Computing	Vikram Patalbansi	MCA	Journal Of Technology	2023	1012-3407	<a href="https://technologyjournal.net/">https://technologyjournal.net/</a>	<a href="https://technologyjournal.net/wp-content/uploads/2023/09/7-JOT1085.pdf">https://technologyjournal.net/wp-content/uploads/2023/09/7-JOT1085.pdf</a>	UGC care
Compound Transmission Security for Mobile Cloud Computing using Spread Spectrum Technique	Vikram Patalbansi	MCA	Journal of Mobile Computing Communications & Mobile Networks	2024	2349-901X	<a href="https://stmcomputers.stmjournals.com/index.php/JoMCCMN">https://stmcomputers.stmjournals.com/index.php/JoMCCMN</a>	<a href="https://stmcomputers.stmjournals.com/index.php/JoMCCMN/article/view/733">https://stmcomputers.stmjournals.com/index.php/JoMCCMN/article/view/733</a>	UGC Care II





# Protecting Data on Mobile Cloud Computing

Vikram Patalbansi, G. Prasanna Laxmi



**Abstract**— Mobile Cloud Computing is a combination of general Cloud Computing and Mobile Computing in which we have to access resources from the remote cloud data center with the help of mobile electronics and peripherals like mobile smartphones, laptops, gadgets, etc. via Cellular Technology or Wireless Communication. Mobile devices have lots of resource constraints like storage capacity, processing speed, and battery life. Hence through simple mobile computing software and programming, we cannot manipulate on mobile devices of cloud data center information. Because of such kinds of difficulty, we have to process information or data through external mobile devices. Accessing and processing of data with the help of Trusted Third Party Agency (TPA) outside the cloud data center and mobile devices have lots of security challenges. To make cloud data secure over outside resources, lots of terminologies and theory are put forward by various researchers. In this paper, we will analyze their theory and its limitations and offer our security algorithm proposal. In this thesis article, we analyze the security framework for storing data on Cloud Server by Mobile and limitation of this process. Also, we review the theory of how data can be secure our data on cloud administrators.

**Keywords:** Mobile Cloud Computing, Security algorithm of cloud, Wireless security

## 1. INTRODUCTION

The Mobile Cloud Computing is hybrid technology in the sense of wireless communication between mobile device and cloud data storage system through cellular technology. Using Mobile Cloud Computing (MCC) all the processing and storage are happen over cloud computing area instead of mobile device due to its limitation in storage and processing power and information are stored in multiple location so that MCC is a reliable system and on-demand we can get access to any information irrespective of location and hardware configuration of user mobile electronic devices and hence sharing of information between two or more entities via wireless communication face more security challenges like phishing attacks, man-in-middle attack, denial-of-service (DoS) etc. The objective of this thesis paper is to propose a new theory of encrypting the information as well as authentication of the mobile user.

Manuscript published on 30 September 2019.

\*Correspondence Author(s)

Vikram Patalbansi, Assist. Professor, L.B.H.S.S.T's ICA Bandra Mumbai  
Research Scholar Pacific University Udaipur. Email:  
vikrampatalbansi14@gmail.com

Dr. G. Prasanna Laxmi, WOS – A Program(DST), Trainer, HMI  
Engineering Services. Email: prassanalaxmigandi@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Retrieval Number: K25740981119/19@BEIESP  
DOI: 10.35940/ijitee.K2574.0981119  
Journal Website: [www.ijitee.org](http://www.ijitee.org)

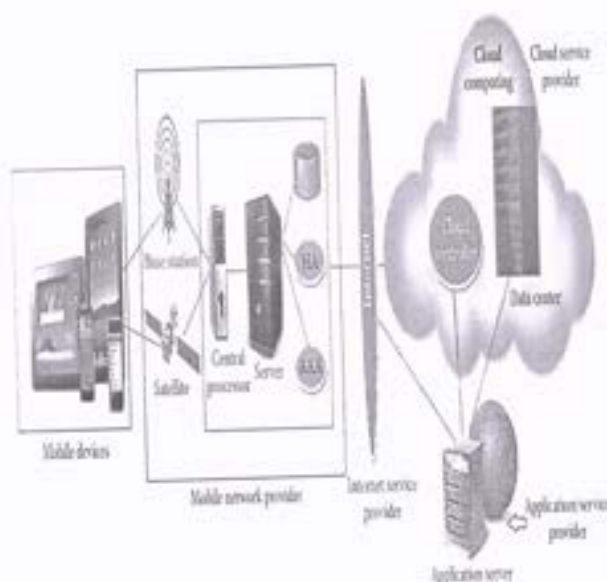


Fig. 1 Mobile Cloud Computing Architecture [4]

## 2. RELATED WORKS

[1] In Mobile Cloud Computing, all small portable devices are wirelessly connected with the cloud server. During wireless communication, the cloud server generates master keys for every mobile device based on their unique identity like MAC address and IMEI etc. After mutual authentication and registration, the mobile devices and cloud server communicated to each other by encrypting information with the help of cloud server, the generated master keys for specific mobile devices. The main limitation of this paper is that mobile devices having geographical area constraint and lack of central standard authenticator. If devices move from one area to another, then it has to be authenticating with a new server and may face problems of compatibility in term of hardware configuration and software. [2] In this papers authors suggested the theory of Cloud-Radio Access Network (C-RAN) to make communication between the mobile device and cloud server with the help of middle man radio base station with high radio signal bandwidth. The C-RAN network architecture has a three-layer model as L1, L2, L3. L1 is the physical layer (PHY), which mainly provides a data transmission service to the higher layers, channel coding, rate matching and Multiple Input Multiple Output (MIMO) technology, etc. L2 is the layer responsible for Media Access Control (MAC), Radio Link Control (RLC) and Packet Data Convergence Protocol (PDCP) that mainly provides data link control



Published By:  
Blue Eyes Intelligence Engineering  
and Sciences Publication (BEIESP)





## Authentication Theory for Mobile Cloud Computing

Vikram Patalbansi  
Department of Computer Science  
Pacific University, Udaipur, India

Dr. G. Prasanna Laxmi  
Department of Computer Sciences Engineering  
Andhra University, India

**Abstract-** Mobile Cloud Computing (MCC) is a hybrid technology of mobile computing, cloud computing, and wireless cellular technology. With the help of mobile devices like smartphone, laptop, iPod, etc., we can access and process remote data which are stored over the cloud server in real-time through wireless networks. Hence it is lots of chances that sensitive information is susceptible to various types of attacks and anyone can misuse our information. So to establish secure transmission of data among various communicating entities of mobile cloud computing, there must be a good quality authentication scheme that should be implemented. Here in the thesis paper, we review the various authentication scheme proposed by various researchers. After studying various protocols we propose our multi factors anonymous authentication scheme under mobile cloud computing network architecture. In the proposed thesis paper, we used the Fuzzy Extractor function is biometric-based key production technology. To manipulate various multiple authentication parameters like userID, password, IMSI, IMEI, virtual smart card, and UICC, authentication application (Mobile App software) is used over mobile devices and established the session with the cloud server. So our scheme avoids any information disclosure even fingerprint impression also and protects mobile client privacy and improves the security of every entity of Mobile Cloud Computing.

**Keywords –** Mobile Cloud Computing, authentication, wireless security.

### I. INTRODUCTION

The combination of cloud infrastructure and mobile technology or cellular network developed a new computational paradigm model called Mobile Cloud Computing (MCC). In MCC network architecture, resource-constrained electronic mobile devices can utilize computational or storage space resources of cloud server or data center via wireless communication network any time or anywhere else locations. [8] Generally any electronics mobile devices become a major part of our life due to its sharing of information in a flexible manner over mobile wireless network. [7] In the Mobile Cloud Computing (MCC) environment, mobile devices access the resource from the cloud server. Hence before getting any kind of service from wireless networks and cloud servers, the mobile devices must be registered and authenticated. As we know mobile devices having resource and computational constraints, so it is not suitable to perform complex operations in the mobile device for authentication purposes. [11] In MCC, if mobile user and cloud service provider are, both registered with the mobile wireless network and after that mobile device and cloud server will be authenticating to each other with unique authentication protocol to establish secure communication between mobile devices and cloud servers over secure channels at both ends to avoid any vulnerabilities and to ensure the legitimacy of data access.

The research paper is organized as follows. Section "Related Works" describe the related works of different authors in various research papers. In the "Proposed System" section we developed the multifactor authentication scheme. And "Security Analysis" describes the advantages of our protocol. Finally, the "Conclusion" section concludes this paper.

### II. RELATED WORK

In our proposed scheme, we are going to improve the security of Mobile Cloud Computing by proposing advanced lightweight bio-metric based multi-factors anonymous authentication scheme under mobile cloud computing network architecture. [1] During communication in Mobile Cloud Computing (MCC) network architecture, it is necessary to implements secure and private communication protocol to make all entities involved in communicating authenticated and attacks full proof. All the information is transmitted over wireless medium including all mobile devices as well as server-related information are in the form of wireless signals, hence it is so hard to ensure that any unauthorized entities or hackers can get access to transmitted or communicates with any devices involved in MCC network architecture and can steal the private or secret information. So it is a challenge to



# Mobile Cloud Computing Cryptographic Scheme

<sup>1</sup>Vikram Patalbansi <sup>2</sup>Dr. G. Prasanna Laxmi

<sup>1</sup>Research Scholar Pacific University, Udaipur India

<sup>2</sup>Faculty, Andhra University, India

<sup>1</sup>vikrampatalbansi14@gmail.com,

<sup>2</sup>prassnalaxmigandi@gmail.com

## Abstract

The ubiquitous network like Mobile Cloud Computing (MCC) provides the high quality of wireless services depending upon the wireless communication system network security level. And so many researches are carried out by the researcher on security algorithms for wireless communication system constructed in different network reliability. In our proposed thesis paper, on a theoretical basis, we developed the theory of MCC Security Layer Protocol security system in which we used the cryptographic hash function SHA-256 to generate a private key for entities, RC5 encryption, and decryption algorithm, Temporal Key Integrity Protocol (TKIP) generating a dynamic sequential key and CRC-32 checksum to detecting the error in our packets. The MSLP uses the stored symmetric secret key calculated on the basis of the Diffie-Hellman Key sharing scheme to generate keystream for cryptography functions. The secret key stored in the device's filesystem our database prior to the deployment on Mobile Cloud Computing and remains the same throughout the session of communication. These systems use the dynamic initialization vector to avoid replay attacks and message integrity code calculated on source and destination devices addresses and actual frame contents. In the proposed thesis paper we analyze the security measures at MSLP level and before transmitting information over the mobile networks, the information is encrypted in the form of frames and at the physical layer, this frame converted into its equivalent radio signals.

**Keyword:** Mobile Cloud Computing, mobile network security, wireless signal security algorithm

## INTRODUCTION

The Mobile Cloud Computing (MCC) consists of individual mobile phone, laptop, or any other electronic devices which are connected with cloud server via the cellular network. Both the entities mobile devices and cloud server shares resources and information to each other over the wireless communication. The need for security in MCC, which arises from the transmission to receiving of secured information. Due to the broadcast nature of the wireless radio channels, anyone can monitor or access wireless communication. In addition to the myriad vulnerabilities of the conventional wired networks, the wireless networks also has a host of the other vulnerabilities associated with the use of radio communication and mobile endpoints. The packets are transmitted over the air link, which makes it relatively easy to eavesdrop, intercept

them, inject malicious payloads or launch Denial of Service (DoS) attacks. [1] Though the cloud communication services providers offer security protection as part of its service and must also take measures to ensure data and information are secure. The fundamental factor defining the success of any new information computing technology is the level of security, it provides to the user. The service provider must fulfill security requirements like confidentiality, integrity, and availability to protect the information in wireless communication.[4] In general, most wireless network receivers devices including all IEEE 802.x protocol compatible devices start to accept messages in the air once a synchronization header (preamble) is detected. They stop receiving messages based on a frame length byte. If collision occurs during the reception of the header, nothing can be received. So to avoid such kind of difficulty proper packet encryption techniques must be used in Mobile Cloud Computing.

## PROPOSED THEORY

[3] In Mobile Cloud Computing (MCC) security issues are divided into three levels viz. Security of mobile devices/terminals, Security of wireless communication channels, and Security of cloud infrastructures. Here in this section, we will discuss security on wireless communication channels. Using Mobile Cloud Computing, mobile users communicate with the cloud servers with the help of communication channels or wireless interfaces. There are lots of possibilities for attackers to break the traditional security arrangements using encryptions techniques or authentications techniques. Because most of the attacker are used to with this techniques and by doing R&D, they can easily do security break up in security arrangements likes access control attacks, confidential attacks,





## Secure Wireless Communication for Mobile Cloud Computing Multimedia Contents

<sup>1</sup>Vikram Patalbansi\* <sup>2</sup>Dr. G. Prasanna Laxmi

<sup>1</sup>Research Scholar Pacific University, Udaipur India

<sup>2</sup>Faculty, Andhra University, India.

### Abstract:

The Mobile Cloud Computing is offering requirements based IT services to mobile user by fetching information from cloud data center throughout worldwide. It also gives the facilities to enables hosting of pervasive applications from customer, consumers, scientific and business domain. The data center or cloud server do not supports automatic leasing of the right amount of services requirements of users while minimizing the cost of leasing or resource allocation and offloading to cloud infrastructures. In this proposed thesis paper we will focus on the following points for secure Mobile Cloud Computing resources scheduling.

1. Architecture principles for automatic management of resource allocation policies and scheduling algorithm during offloading and retrieving the information from cloud data center.
2. Discuss some methodologies on security algorithm during transmission of information over wireless communication mode while offloading and fetching information over cloud server.

### Keywords:

Mobile Cloud Computing, Wireless Signal Security, Network Slicing, Spread Spectrum Technique/

## I. INTRODUCTION

Mobile Cloud Computing (MCC) is an Internet based technology which offering utility oriented IT services to mobile devices users on pay-as-you-go model via distributed virtualized and scalable infrastructure available with number of hosts like task scheduler, virtual machine and proxy server etc. During high demands of mobile users through wireless signals, the workloads on cellular and cloud networks increases which may impact the performance of services due to load imbalance.

To give good Quality of Services (QoS) to users, we have to make proper arrangements in available resources over mobile cloud computing in terms of optimized usage of resources, limiting the operational costs and increasing scalability of wireless and cloud networks infrastructures.

[1] The mobile devices lacks adequate resources like battery power life, storages and processing capabilities. Due to such kinds of limitations user task request to process gets affected. To overcome these kinds of problems, in early 1990's client-server model over network processing was introduces so that high computation-intensive tasks are executed over server side irrespective of client side due its limitation. However, by using distributed computing or parallel computing over cloud network architecture, Mobile Cloud Computing facing many challenges like parameter marshalling, client and service binding, and the semantics of remote invocation and security challenges over wireless network communication.

[2] The authors in this paper raise the points on data transfer size optimization and data persistence versus data availability. During offloading data from mobile devices to cloud infrastructures, how much data to move in a single transfer. In accordance with wireless network bandwidth, we have to optimize the data rate in terms of signals chunk size with uniform parameters requirements in communication to achieve good quality of data transfer. The Data Availability is important for completing tasks in a currently running process. Data persistence refers to storing data in the cloud until it needed again in future. For all of this stuff Mobile Cloud Computing architecture need good signals bandwidth, device capacity and latency in caching of information.

## II. RELATED WORK

[3] Due to the continuous and explosive growth in data traffic in the future, data offloading has become essential in mobile networks in order to decrease the capital expenditure (CPEX) and operational expenditure (OPEX) of mobile network operators (MNOs) while maintaining or enhancing the QoS/QoE of end users.

## Blockchain-Based Multi-Factor Mobile Device Authentication Technique in Mobile Cloud Computing

Mr. Vikram Patalbansi<sup>1</sup>, Dr. Jayshree Jain<sup>2</sup>, Dr. G. Prasanna Laxmi<sup>3</sup>

Research Scholar, Pacific University, Udaipur, India Professor, Pacific University Udaipur

J. Woman Scientist, DST-WISE Postdoctoral.

**Abstract**—Combining general cloud computing with mobile computing, MCC<sup>1</sup> requires the use of mobile electronics and peripherals, such as mobile smartphones, laptops, and other devices, to access resources from a remote cloud data center using cellular technology or wireless communication. Storage space, computing power, and battery life are just a few of the resource limitations that mobile devices in general come across. Therefore, we are unable to manipulate information from cloud data centers on mobile devices using basic mobile computing tools and programming. The process of mobile device authentication involves establishing the legitimacy of the mobile network and cloud computing system to safeguard the user's sensitive data from control orders from unauthorized users or user equipment. Information in the form of radio signals has been experiencing increased security difficulties due to the open nature of wireless networks or cellular networks utilized in mobile cloud computing systems. Mobile device authentication must be necessary to improve the security performance of the wireless system in MCC due to the open nature and susceptibility of wireless communication. In the proposed thesis, we make various identity and access management (IAM) suggestions to control which devices connect and are permitted to access business data from the cloud server via a wireless mobile network, or 5G mobile networks. A blockchain-based authentication system has been developed recently with the rise of blockchain technology to securely confirm user identification in online mode. With the use of blockchain technology, the complete information system network can maintain its data integrity; no external entity is required to centrally monitor the network. The level of security of authorized access to company data, information, and resources from the MCC cloud storage system will be increased by the multi-factor authentication system integrated with blockchain technology. In the proposed thesis, we also mention several research projects on terminology for mobile device authentication utilizing the technology of blockchain.

**Keywords:** Mobile Cloud Computing, multi-factor authentication, wireless network, and blockchain security.

### 1. Introduction

The term "Mobile Cloud Computing," or MCC for short, refers to a new computing paradigm that combines aspects of cloud computing with mobile networks, each of which has a variety of components. The MCC grants access to cloud computing resources, including processing power, storage space and services, for any electronic mobile device. These resources are delivered using wireless communication networks, such as mobile or cellular networks, Wi-Fi<sup>2</sup> [1], and so on. Using Mobile Cloud Computing (MCC), all of the processing and storage is done over the cloud computing area instead of the mobile device due to the mobile device's limitations in storage and processing power, and information is stored in multiple

locations so that MCC is a reliable system and on-demand we can get access to any information regardless of location and hardware configuration of user mobile electronic devices and therefore sharing

of information between two or more entities via the wireless connection [22]. The purpose of this thesis paper is to represent a new theory of encrypting information as well as authenticating the user of a mobile device. Specifically, this study will focus on mobile devices authentication. Because of this, mobile devices need to be registered and authorized before they can get any form of service from wireless networks or cloud servers. Because of the limited resources and processing power that mobile devices have, so it is not advisable to carry out complicated tasks on a





# Packet Cryptography Technique for Data Transit in Mobile Cloud Computing

Mr. Vikram Patalbansi<sup>1</sup>, Dr. Jayshree Jain<sup>2</sup>, Dr. G. Prasanna Laxmi<sup>3</sup>

1. Research Scholar, Pacific University, Udaipur, India  
(Corresponding author:

2. Professor, Pacific University Udaipur

3. Principal & IT Head,  
SDS College of Arts and Applied Science, Shreeramnagar, Vizianagaram District, AP, India

## Abstract

High-quality wireless services are made available via pervasive networks like Mobile Cloud Computing (MCC), but their reliability is contingent on the robustness of the underlying wireless communication system's network security. Many studies have been conducted on the topic of developing security algorithms for wireless communication systems built with varying degrees of network reliability. Our proposed thesis paper details the theoretical development of a security system for the MCC Security Layer Protocol, which makes use of the SHA-256 cryptographic hash function to generate private keys for entities, the RC5 encryption and decryption algorithm, the Temporal Key Integrity Protocol (TKIP) to generate a dynamic sequential key, and the CRC-32 checksum to detect errors in our packets. Using the Diffie-Hellman Key sharing algorithm, the MSLP's stored symmetric secret key is used to generate a keystream for use in cryptographic operations. Before deploying on Mobile Cloud Computing, we save a private key to our database on the device, and that key never changes. To foil reply attacks and message integrity codes based on the addresses of sending and receiving devices and the contents of individual frames, these systems make use of a "dynamic initialization vector." Before data is sent across mobile networks, it is encrypted in the form of frames at the MSLP level and translated into its equivalent radio signals at the physical layer, both of which are analyzed in the proposed thesis paper.

**Keywords:** Mobile Cloud Computing, mobile network security, wireless signal security algorithm, packet cryptography, RC5

## 1. INTRODUCTION

Mobile Cloud Computing (MCC) connects mobile phones, laptops, and other devices to cloud servers over cellular networks. Mobile devices and cloud servers share resources and information wirelessly. The transmission and reception of secure information necessitate MCC security. Wireless communication is broadcast, so anyone may listen in. Wireless networks have radio communication and mobile endpoint vulnerabilities in addition to the many wired network vulnerabilities. Airlink packets are easy to capture and eavesdrop on them, insert malware, or execute DoS attacks. [1] Cloud communication providers must secure data and information as part of their service. New information computing technologies succeed or fail based on user security. Wireless communication requires secrecy, integrity, and availability from the service provider.[4]Once a synchronization header (preamble) is recognized, most wireless network receivers, including IEEE 802. x devices, start accepting airborne messages. Messages halt after a frame

length byte. A collision during header receipt prevents reception. Mobile Cloud Computing needs packet encryption to avoid such issues.

[25]To protect the privacy and authenticity of information sent via a wireless network, a method called "packet cryptography" is employed. Each data packet is encrypted before transmission and decrypted upon arrival. Preventing malicious parties from gaining access to private data in transit is packet cryptography's fundamental goal. If the packets are encrypted, even if an attacker can intercept them, it will be impossible to read the data without the key.

Packet cryptography makes use of a wide range of cryptographic methods and protocols, including both symmetric and asymmetric encryption. In symmetric encryption, a single key serves as both the encryption and decryption for the data packets. The Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) are both examples of symmetric encryption methods. However, in asymmetric encryption, two keys are used: one for encryption and one for decryption. Digital signatures and safe key exchange are two of the extra security features made possible by this technology. Elliptic Curve Cryptography (ECC) and RSA are two popular asymmetric encryption techniques.

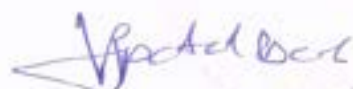
Packet cryptography is used to secure wireless network communications and can be implemented at multiple layers of the network stack, including the network layer (through IPsec) and the transport layer (via TLS or SSL). Factors like as the network protocol in use and the intended level of security inform the decision of which encryption method to employ and at which layer to implement it. When it comes to wireless network communication, packet cryptography is crucial since it safeguards sensitive data from being intercepted while in transit and ensures its authenticity.

Data sent over a wireless network can be encrypted using a method called "packet cryptography." A key feature is its ability to encrypt data packets before their transmission over a network. Because of this, it is considerably harder for hackers to intercept the data and decipher it. Numerous methods of packet encryption are now in use. Some of the most typical examples include:

[23]Data Encryption Standard (DES) is a 56-bit key symmetric encryption technique. Although it has a poor reputation for strength, it finds widespread use.

The 128-bit, 192-bit, or 256-bit keys used by AES, the Advanced Encryption Standard, make it a symmetric encryption technique. It is the most used method of packet encryption because of its high level of security and widespread adoption.

[23]To encrypt data, public-key cryptography (PKC) employs



# JOURNAL OF MOBILE COMPUTING, COMMUNICATIONS & MOBILE NETWORKS

[Submissions](#) [Current](#) [Archives](#) [Old Archives](#) [Author](#) [Announcements](#) [About](#) [Q Search](#)

[Home](#) / [Archives](#) /  
Vol. 10 No. 3 (2023): Journal of Mobile Computing, Communications & Mobile Networks /  
[Review Article](#)

## Compound Transmission Security for Mobile Cloud Computing Using Spread Spectrum Technique

**Vikram Patalbansi**

Research Scholar, Department of Computer  
Engineering, Pacific Academy of Higher  
Education and Research University (PAHER),  
Udaipur, India

**Jayshree Jain**

Professor, Department of Computer  
Engineering, Pacific Academic Higher  
Education and Research University, Udaipur,  
India

**G. Prasanna Laxmi**

 PDF

Published

2024-01-11

Issue

Vol. 10 No. 3 (2023): Journal of Mobile

Computing, Communications & Mobile  
Networks





## A COMPARISON AND ANALYSIS OF SUPERVISED MACHINE LEARNING ALGORITHMS TOWARDS ACCURATE PREDICTING OF HEART DISEASES

Dr. Prashant Sharma <sup>1</sup>, Avantika Mahadik <sup>2</sup>, Dr. Vaibhav Narawade <sup>3</sup>

<sup>1</sup>Associate Professor, Department of Computer Science and Engineering,  
Pacific (PAHER) University Udaipur, Rajasthan, India

<sup>1</sup>[prashant.sharma@pacific-it.ac.in](mailto:prashant.sharma@pacific-it.ac.in)

<sup>2</sup>Research Scholar, Pacific (PAHER) University Udaipur, Rajasthan, India

<sup>2</sup>[avantika\\_mahadik@rediffmail.com](mailto:avantika_mahadik@rediffmail.com)

<sup>3</sup>Professor, Department of Computer Engineering, Ramrao Adik Institute of Technology

<sup>3</sup>[vaibhav.narawade@rait.ac.in](mailto:vaibhav.narawade@rait.ac.in)

**Abstract:** In machine learning, forecasting is one of the most significant applications. Machine learning uses various techniques for prediction. Taking into consideration the recent work, we are focusing on machine learning algorithms and analysing how these algorithms are used in the healthcare industry to predict heart diseases. In supervised machine learning, the machine first states the patterns from labelled dataset (training dataset) and secondly it applies that on the unlabelled dataset (testing dataset) to predict the result. The training dataset includes input and correct output. Classification and Regression are the two techniques used in supervised machine learning. Classification technique is very commonly used to predict diseases in healthcare. Classification is a learning technique in which, deciding of class label to a given data done through machine learning algorithms. Regression technique shows the relationship between two or more variables. We discover links between dependent and independent variables through regression techniques.

The core focus of this exploration is to conduct a systematic proportional study and examine of four machine learning algorithms, specifically random forest, support vector machine, KNN and decision tree in heart disease prediction. We found that support vector machine and random forest provides the highest accuracy in the prediction of heart disease among all. Random forest can be integrated with another classifier to achieve more efficiency.

**Keywords:** Machine learning, random forest, decision tree, Support vector machine, KNN and Heart Disease,

### Introduction:

Nowadays, various industries in public and private sectors generate vast quantity of data. Data is a key aspect and plays a vital role in new development. We need reliable information to produce optimized and best outcomes in any area. Data in an appropriate structure, organized manner and in a suitable predefined model is called structured data. Unstructured or raw data tend to give rise to several problems while working with them, especially if that data is used in analysis. Today healthcare industry is one of the biggest industries which has a huge amount of medical data. This industry collects the data from various sources like hospitals, insurance companies, pharmaceutical industries, Epidemiological Surveillance, census, other health records, sample registration system, patient's disease registries, electronic health record and clinical surveys. The collected data is stored and used for analysis for better improvement in the medical field, research in drugs and predication or diagnosis of disease. Medical data comes in many forms. Text, images, sound, various readings from wearable medical IoT devices, biosensors data, data collected from clinical instruments and devices



## PREDICTION AND ANALYSIS OF DIABETES USING MACHINE LEARNING

**Avantika Mahadik**

Research Scholar, Pacific(PAHER) University Udaipur

avantika\_mahadik@rediffmail.com

**Dr. Prashant Sharma**

Associate Professor, Department of Computer Science and Engineering, Pacific(PAHER)

University Udaipur, prashant.sharma@pacific-it.ac.in

**Dr. Vaibhav Narawade**

Professor, Department of Computer Engineering, Ramrao Adik Institute of Technology, Navi

Mumbai, vaibhav.narawade@rait.ac.in

**Abstract** - Diabetes is a chronic condition that results from the body's resistance to or the pancreas' inability to effectively use the insulin it produces. Insulin, a peptide hormone, was responsible for regulating blood sugar. Repeated episodes of hyperglycemia, also known as high blood glucose or elevated blood sugar, are caused by hysterical diabetes and may cause severe damage to a variety of unique human body systems, including the nervous and cardiovascular systems. Long-term diabetic nerve, eye, renal, vascular, cardiovascular, and visual impairments are real. Adults with diabetes are two to three times more likely to have a heart attack or stroke. The likelihood of a negative result from several viral infections, including COVID-19, is raised in people with diabetes. One in five of the more than 58 million persons who live with diabetes are unaware of their condition. Different diseases are identified using machine learning methods, including Decision Trees (DT), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN). The use of machine learning algorithms can result in quick and accurate disease prediction. One of the well-liked machine learning techniques in the medical industry is the decision tree, which has strong categorization capabilities. The most important risk factors for prediabetes were discovered to be age, waist-hip ratio (WHR), BMI, systolic and diastolic blood pressure, and a family history of diabetes. While the classification accuracy of the images produced by both methods is satisfactory, the SVM greatly outperforms the KNN in terms of classification speed and accuracy. SVM offered 98% accuracy, which is higher than DT (92.4%) and KNN (93.94%). Glucose plays a major role in diabetes.

**Index Terms** - Prediction, Diabetes, Machine Learning.

**I. INTRODUCTION**

The worldwide healthcare system may face a catastrophe because of diabetes, a long-term ailment. The metabolic disorder known as diabetes [1], or diabetes mellitus, is characterized by persistently high levels of blood sugar. The number of people living with diabetes is expected to rise from the current 522 million in 2022 (up from 108 million in 2000) [2]. As a whole, the rate of increase has been higher in low and medium income





## **Proficient Prognostication through Hybrid Approach for Heart Disease**

**By**

**Avantika Mahadik**

Research Scholar, Pacific (PAHER) University, Udaipur, India

Email- [avantika\\_mahadik@rediffmail.com](mailto:avantika_mahadik@rediffmail.com)

**Dr. Prashant Sharma**

Associate Professor, Department of Computer Science and Engineering Pacific (PAHER) University, Udaipur, India

Email- [prashant.sharma@pacific-it.ac.in](mailto:prashant.sharma@pacific-it.ac.in)

**Dr. Vaibhav Narawade**

Professor, Dr. D Y Patil's Ramrao Adik Institute of Technology, Maharashtra, India

Email- [vaibhav.narawade@rait.ac.in](mailto:vaibhav.narawade@rait.ac.in)

### **Abstract**

Machine learning uses variations of methods for disease prediction. The present article is aiming to give a thorough explanation of how random forest, decision tree, liner regression are used in our research, especially when combined and applied for the heart disease prognosis. The outcomes of an experiment comparing the implementation of forecasting techniques on the same dataset. In our research, we independently experimented the dataset with random forest, decision tree, and linear regression. The DTKNN<sup>1</sup> is our proposed model where we hybrid two machine learning algorithms for achieving the highest accuracy for heart disease prediction. 303 records and 1025 records from different regions combined together in the DTKNN to get 100% accuracy in the prediction of heart disease. In our article we compared DTKNN with other machine learning algorithms. Based on the outcomes of our experiments and analysis, we can accomplish that planned model generated the uppermost accurateness (100%) when using decision tree and KNN together.

**Keywords:** Heart Disease, Machine learning algorithms, Boosting, Ensemble classifier

### **Introduction**

An enormous amount of data is generated in today's public and business sectors world. Data is important and essential to new development. To achieve the greatest and most optimised results in any sector, we need trustworthy information. Structured data is data that has an adequate specified model, a proper structure, and organisation. Working with unstructured or raw data frequently results in a number of issues, particularly if that data is used for analysis [19].

Today, healthcare sector is known as the largest sector which has a gigantic amount of medical data. This industry collects the data from various sources like hospitals, insurance companies, pharmaceutical industries, Epidemiological Surveillance, census, other health records, sample registration system, patient's disease registries, electronic health record and

<sup>1</sup> DTKNN- Decision Tree and K-nearest Neighbour





# A Summary of Comparative Study of Software Reliability

Ms Rashmita Pradhan  
Research Scholar, Mewar University

Dr Amit Gupta  
Associate Professor, Maharaja Agrasen Institute of Technology

**Abstract**—With the combination of informatisation and industrialisation, software utilisation has become more extensive and plays a crucial role in many facilities. At the same time, Software failures cause huge losses, thus ensuring the reliability of software becomes increasingly necessary. The fundamental conceptions of software reliability are put ahead in this paper, and comparative analyses on the research status at home and abroad are studied. Meanwhile, the prospect of further progress of software reliability is made.

**Keywords**- software reliability; synthesis of informatisation and industrialisation; comparative analysis

## Differences between Hardware Reliability and Software Reliability

A large section of hardware failure is due to material wear and material ageing, while software will not increase over time, namely never wear.

The critical portion of hardware reliability is present, affected by design, production, and service. Nonetheless, source code is an essential part of software reliability. As for embedded software, the interface's fault within hardware and software is a significant factor in failing [2].

## C. Importance of Software Reliability

### 1) Software reliability is a necessary condition to support regular system operation

The effect of software is getting more and more important as a growing number of digital devices are putting into use. In the aerospace domain, the scale of source code in airborne software gives a million lines. However, the sharp rise of scale and complexity in the software also improves the failure number. One study shows that professional software developers' codes would have six errors every thousand lines [3]. Following this fault occurrence, software with a million line codes would produce as many as 6000 faults. What is more serious, the depth of fault increases geometrically as the range of software grows. The increasing number of faults makes mistake location more complex, and the repair cost rise dramatically. Besides, software breakdown can cause serious consequences. The most notable examples are: in 1962, MARINER I conducted by the United States to Venus lost control 293 seconds after staying launched. NASA owed this fault to the wrong code line in the Fortran language, causing the cost loss as high as 80 million dollars. The popular safety company SecurityFocus data reveals that the most severe power blackout occurred in the United States and Canada on August 14th, 2003, following software failure. Serious events caused by software failure are by no agency, only these two. These accidents show us a lesson that software reliability needs to be analysed before devices are put into use.

### 2) Software reliability becomes the bottleneck to improve system reliability

Software plays an increasing part in systems. For example, every time the fighter aircraft updates a new generation, the functions realised by software double [3]. Software reliability is directly related to system reliability.

## I. INTRODUCTION

Now, software plays a more critical role in more industries. However, with modern industrial operations growing more complex, assurance of software reliability becomes more complicated. Although many kinds of research should be carried out and plenty of applications have been put into use, there is still a long way to go in software reliability.

## DEFINITION AND IMPORTANCE OF SOFTWARE RELIABILITY

### A. Definition

IEEE Computer Society enacted a clear definition of software reliability in 1983, which was believed as a national model by the National Institute of Standards and Technology (NIST) in the United States. Following the year 1989, China also took the comment as a national standard. According to GB/T 11457-95-Software Engineering Terms, the meaning of software reliability is as follows [1]:

- Software reliability is the possibility of failure-free software operation for a specified period below a specified condition. This probability uses the input and usage of the way and the failure that existed in software. The system input will decide whether an existing loss will be found.
- Software reliability is how the software does the required functions during the prescribed period under a specified condition.





# OPTIMAL ESTIMATION OF SOFTWARE RELIABILITY WITH NEURAL FUZZY MODEL

Rashmita Pradhan

Research Scholar, Mewar University

## ABSTRACT

Software reliability is defined as the probability of software to deliver correct service over a period of time under a specified environment. This is becoming more and more important in various software organizations to discover the faults that occur commonly during development process. As the demand of the software application programs increases the quality becomes higher and higher and the reliability of these software becomes more essential. Hence Software reliability is mentioned to be as the one of the important factor during development. Many analytical models were being proposed over the years for assessing the reliability of a software system and for modeling the growth trends of software reliability with different capabilities of prediction at different testing phases. A Neuro Fuzzy based software reliability (SR) model is presented to estimate and assess the quality. Multiple datasets containing software failures are applied to the proposed model. These datasets are obtained from several software projects. Then it is observed that the results obtained indicate a significant improvement in performance by using neural fuzzy model over conventional statistical models (Fuzzy Model) based on non-homogeneous Poisson process.

## 1. INTRODUCTION

### 1.1 Background

Dependency on computer aided systems is increasing rapidly day by day and the software systems operating in it. However this quality of service by the system is degraded by some software failures or fails to meet the required level of performance this make many of the people to strike off these software. This model attempt to match product properties with the software quality attributes. Hence if a company is to develop high quality software, it is important

to employ some efforts on software reliability and usability. However, this thesis focuses only on software reliability based models.

### 1.2 Software Reliability

The American Institute of Aeronautics and Astronautics (AIAA) defines SRE as "the application of statistical techniques to data collected during system development and operation to specify, predict, estimate, and assess the reliability of software-based systems"[8]. Three kinds of identifiers for Software Reliability. They are a) Probability of failure free operation over a specified time interval. b) Mean time to failure (MTTF) the predicted elapsed time between inherent failures of a system during operation. c) Expected number of failures per unit time interval termed failure intensity.

Here in our work, a Neuro Fuzzy based SRGM is proposed. In order to test the accuracy of proposed model, real failure data of a software project is required. However, it is a very time consuming process to carryout software testing for a real project and could even take years. This is not feasible within the available time and thus secondary data which have already been collected and published.

### 1.3 Neuro Fuzzy Models

The idea of a Neuro Fuzzy system is to find the parameters of a fuzzy system by means of learning methods obtained from neural networks used to train the system. They cannot be applied directly to a fuzzy system, because the functions used in the inference process are usually not differentiable. There are two solutions to this problem: a) Replace the functions used in the fuzzy system (like min and max) by differentiable functions, or b) Do not use a gradient-based



# IMPROVED SOFTWARE RELIABILITY GROWTH MODEL FOR FUZZY ENVIRONMENT

Rashmita Pradhan

Research Scholar, Mewar University

## Abstract

Software is often a key component of the high technology systems that are so common in modern society. High reliable software is critical both to software industries and the end users of the developed software, and also for the social community generally, because failures of software can cause major disruption to business and can even threaten emergency service. It is a challenge to be able to enhance the quality of a model early enough to prevent problems from fault later in the life cycle because it is much more cost-effective to correct software faults early in the development process than later when they cause failure. This is why building software reliability growth models have gained considered importance in assessing reliability of software products. In our paper, we proposed an approach for assessing the software reliability by using different machine learning techniques like neural-networks, fuzzy logic etc., to measure the software errors to improve the Software Reliability at different phases of Software Development Life Cycle(SDLC).

**Keywords (Size 10 & Bold) —** Software Reliability, Neural Networks, Fuzzy Systems, Fault, Software Development Life Cycle(SDLC), Software Reliability Growth Models(SRGMS)

## I. INTRODUCTION

Software Reliability is defined as the probability of failure-free operation of the software over a specified period of time in a specified environment[1]. One approach proposed by Brocklehurst et al.(IEEE Trans. on Software Engineering, 1990) is to try a set of models and selecting the one that best suits the situation. This is a trial and error procedure/head and tail procedure for assessing the software reliability at different phases of software Development Life Cycle(SDLC). It was claimed that the different models have different predictive capabilities at different phases of software testing life cycle and there is no single model that can be relied on for accurate prediction in all circumstances for all different phases of Software Development Life Cycle(SDLC) (Whitley et al. IEEE Tran. on Software Engineering, 1992).Whitley et al. (IEEE Tran. on Software Engineering, 1992) specified that," the problem of selecting a model can be addressed in two ways[2]:

- 1) By generalizing the applicability of software reliability growth models by analyzing their predictability across a broad spectrum of representative data sets.
- 2) By developing adaptive models, nevertheless, the issue of generalization still remains as an open issue".

