



**Bahria University**  
Discovering Knowledge

**FINAL YEAR PROJECT REPORT**  
**USER AUTHENTICATION SCHEME FOR**  
**MOBILE CLOUD COMPUTING**

**By**

<b>FILZA ATIF</b>	<b>(43695)</b>
<b>BILAL AHMED TOOR</b>	<b>(43757)</b>
<b>OSAMA BIN ZAHID</b>	<b>(43784)</b>

**SUPERVISED BY**  
**(DR. GHULAM SHAIKH)**

**BAHRIA UNIVERSITY (KARACHI CAMPUS)**

**2019**

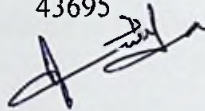
## DECLARATION

We hereby declare that this project report is based on our original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at Bahria University or other institutions.

Name : FILZA ATIF

Reg No. : 43695

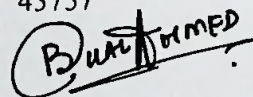
Signature :



Name : BILAL AHMED TOOR

Reg No. : 43757

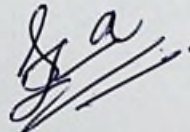
Signature :



Name : OSAMA BIN ZAHID

Reg No. : 43784

Signature :

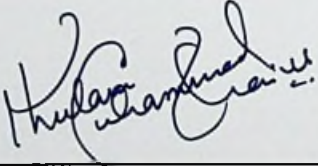


Date : 16<sup>th</sup> DECEMBER 2019

**APPROVAL FOR SUBMISSION**

We certify that this project report entitled **“USER AUTHENTICATION SCHEME FOR MOBILE CLOUD COMPUTING”** was prepared by **FILZA ATIF, BILAL AHMED TOOR** and **OSAMA BIN ZAHID** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Computer Science at Bahria University.

Approved by,

Signature :  \_\_\_\_\_

Supervisor: Dr GHULAM MUHAMMAD SHAIKH

Date : 16<sup>th</sup> December 2019

## ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express our gratitude to our research supervisor, Dr. Ghulam Muhammad Shaikh for his invaluable advice, guidance and his enormous patience throughout the development of the research.

In addition, we would also like to express our appreciation for our loving parents and friends who had helped and given us encouragement.

## USER AUTHENTICATION SCHEME FOR MOBILE CLOUD COMPUTING

### ABSTRACT

The key objective of this project is to develop an effective authentication scheme through which users can verify their identities on a mobile cloud computing platform and gain the authentication necessary to access the system and then the data that concerns them. This report elaborates the various mechanisms considered and used for the authentication scheme and the end result of the research will be a demonstration of how the authentication scheme can be used to secure data in a mobile cloud computing environment while only giving access to users who can authenticate themselves.

Authentication refers to the process of verifying the credibility and validity of a certain entity and, in this context of this project, data authentication refers to the process of verifying a user's identity and, based off this verification, giving them access to the data that they require or is linked to their credentials.

The project takes into consideration various different authentication schemes that have been already been developed such as 2FA (2 Factor Authentication), Multi Factor Authentication, OTP (One Time Password). In order to provide a high level of security to users, the goal is to research a single effective authentication scheme through which users can get access to all the mobile cloud computing services they require.

Another significant benefit of this research is that, by removing unnecessary complexities from the authentication process and making it revolve around a singular key, authentication methods will require significantly less resources than they usually do thereby improving the speed at which users can authenticate themselves.

## TABLE OF CONTENTS

<b>DECLARATION</b>	<b>ii</b>
<b>APPROVAL FOR SUBMISSION</b>	<b>iii</b>
<b>ACKNOWLEDGEMENTS</b>	<b>vi</b>
<b>ABSTRACT</b>	<b>vii</b>
<b>TABLE OF CONTENTS</b>	<b>viii</b>
<b>LIST OF FIGURES</b>	<b>xi</b>
<b>LIST OF SYMBOLS / ABBREVIATIONS</b>	<b>xii</b>

### CHAPTERS

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	1.1 Background	1
	1.2 Problem Statements	2
	1.3 Aims and Objectives	2
	1.4 Scope of Project	3
<b>2</b>	<b>LITERATURE REVIEW</b>	<b>4</b>
	2.1 Introduction	4
	2.2 Current Authentication Schemes	4
	2.2.1 Two Factor Authentication	5
	2.2.2 Single Sign On	6
	2.2.3 Biometric Authentication	7
	2.2.4 One Time Password	9
	2.2.5 Hybrid Authentication	10
	2.3 Potential Risks of Mobile Cloud Computing	11
	2.3.1 Unauthorized Access to Sensitive Data	11

2.3.2	Inconsistent Availability	11
2.3.4	Risks at the Vendor End	12
2.4	Potential Threats to Mobile Cloud Computing	13
2.4.1	Packet Sniffing	13
2.4.2	DoS/DDoS	14
2.4.3	Man in the Middle	14
2.4.4	Data Breaches	15
2.5	Benefits of Mobile Cloud Computing	16
2.5.1	On Demand Data Access	16
2.5.2	Reduced Operational Costs	17
2.5.3	Improved Scalability	18
2.5.4	Storage as a Service (StaaS)	18
2.5.5	Infrastructure as a Service (IaaS)	19
2.6	Applications of the System	20
2.6.1	Applications in the Business Sector	20
2.6.2	Applications in Educational Institutes	21
2.6.3	Applications in Military	22
2.7	Future of Mobile Cloud Computing	23
2.7.1	Future Challenges for Mobile Cloud Computing	23
2.7.2	Future Opportunities for Mobile Cloud Computing	24
<b>3</b>	<b>DESIGN AND METHODOLOGY</b>	<b>25</b>
3.1	Authentication Scheme Being Used	25
3.2	System Functionality	26
3.3	System Requirements	29
3.3.1	Hardware	29
3.3.2	Software	29
3.4	Why we Aren't Using Built-in Fingerprint Sensors	30

<b>4</b>	<b>IMPLEMENTATION</b>	<b>31</b>
4.1	System Specifications	31
	4.1.1 Fingerprint Reader	31
	4.1.2 Cloud Service	33
4.2	Coding and Development	34
	4.2.1 Permissions Function	34
	4.2.2 Acquiring and Storing Fingerprints	35
	4.2.3 Saving Data to Firebase	36
	4.2.4 Converting Fingerprint Data to Grayscale	37
4.3	How the System is Operated	38
	4.3.1 Registration	38
	4.3.2 Logging In	39
4.4	Interface	40
	4.4.1 Sign Up Menu	41
	4.4.2 Fingerprint Registration at Signup	42
	4.4.3 Login Menu	43
	4.4.4 Fingerprint Authentication at Login	44
<b>5</b>	<b>RESULTS &amp; DISCUSSION</b>	<b>45</b>
5.1	Preliminary Testing, Results and Discussion	45
5.2	Observation and Further Discussion	46
<b>6</b>	<b>CONCLUSION</b>	<b>47</b>
6.1	Results	47
6.2	Advantages of the Proposed System	48
6.3	Disadvantages of the Proposed System	49
6.4	Future Improvements	49
	<b>REFERENCES</b>	<b>50</b>
	<b>APPENDICES</b>	<b>54</b>