



**FINAL YEAR PROJECT REPORT**

**SMARTPHONE-BASED ATTACKS AGAINST 3D  
PRINTERS, ANALYSIS AND PREVENTION  
USING IOT SYSTEMS**

**In fulfillment of the requirement  
For degree of  
BS (COMPUTER SCIENCES)**

**By**

**SYED HAMZA BARI**

**48421 BSCS**

**SYED M. MUSTUFA RIZVI**

**48548 BSCS**

**HAMMAD AHMED**

**48506 BSCS**

**SUPERVISED**

**BY**

**SIR IMRAN MEMON**

**BAHRIA UNIVERSITY (KARACHI CAMPUS)**

**FALL-2020**

## 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.

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


Name : Sved Humza Bari

Reg No. : 48421

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

Name : Hammad Ahmed

Reg No. : 48506

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

Name : Syed Muhammad Mustufa Rizvi

Reg No. : 48548

Date : 08-01-21

**APPROVAL FOR SUBMISSION**

We certify that this project report entitled "**Smartphone-based Attacks Against 3D printers, analysis and prevention using IOT systems**" was prepared by **Syed Humza Bari, Syed Muhammad Mustufa Rizvi and Hammad Ahmed** 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: Sir Imran Memon

Date : 14<sup>th</sup> December 2020

## ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express my gratitude to my research supervisor, Imran Memon for his invaluable advice, guidance and his enormous patience throughout the development of the research.

In addition, we would also like to express my gratitude to our loving parent and friends who had helped and given me encouragement.

## Smartphone-based Attacks Against 3D printers, analysis and prevention using IOT systems

### ABSTRACT

Human beings cannot be happy with any kind of tiredness based work. so they focused on machines to work on behalf of humans. The Internet-based latest technology provides the platforms for human beings to relax and unburden feeling. The Internet of Things (IoT) field efficiently helps human beings with smart decisions through Machine-to-Machine (M2M) communication all over the world. It has been difficult to ignore the importance of the IoT field with the new development of applications such as a smartphone in the present era. The IoT field sensor plays a vital role in sensing the intelligent object/things and making an intelligent decision after sensing the objects. The rapid development of new applications using smartphones in the world caused all users of the IoT community to be faced with one major challenge of security in the form of side channel attacks against highly intensive 3D printing systems. The smartphone formulated Intellectual property (IP) of side channel attacks investigate against 3D printer in the physical domain through reconstructed G-code file through primitive operations. The smartphone (Nexus 5) solved the main problems such as orientation fixing, model accuracy of frame size and validate the feasibility and effectiveness in real case studies against the 3D printer. The 3D printing estimated value reached 20.2 billion of dollars in 2021. The thermal camera is used for exploring the side channel attacks after reconstructing the objects against 3D printers. The researcher analyzed IoT security relevant issues which were avoided in future by enhanced strong security mechanism strategy, encryption, and machine learning-based algorithms, latest technologies, schemes and protocols utilized in an efficient way.

## TABLE OF CONTENTS

DECLARATION	ii
APPROVAL FOR SUBMISSION	iii
ACKNOWLEDGEMENTS	vi
ABSTRACT	vii
TABLE OF CONTENTS	viii

### CHAPTER

1	INTRODUCTION	10
	1.1 Background	10
	1.2 Problem Statements	10
	1.3 Aims and Objectives	11
	1.4 Scope of Project	11
2	LITERATURE REVIEW	12
3	DESIGN AND METHODOLOGY	16
4	IMPLEMENTATION	21
	4.1 FEW ATTACK TYPES	
5	RESULTS AND DISCUSSIONS	31
	5.1 Result	
	5.2 Discussions	

<b>6</b>	<b>CONCLUSION AND RECOMMENDATIONS</b>	<b>41</b>
6.1	Conclusion	
6.2	Recommendation	
	<b>REFERENCES</b>	<b>43</b>