ISSN 2820-2147

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTING

VOLUME 01 , ISSUE 02 JULY 2022

IJRC

International Journal of Research in Computing (IJRC)

Volume 01 Issue 02

July 2022

ISSN 2820-2147

Published by

Faculty of Computing, General Sir John Kotelawala Defence University,
Ratmalana, Sri Lanka

Tel: +94-11-2635268
e-Mail: editor@ijrcom.org & journal.foc@kdu.ac.lk
Website: http://ijrcom.org/

EDITORIAL COMMITTEE

MEMBERS OF THE EDITORIAL BOARD

Faculty of Computing
General Sir John Kotelawala Defence University

Ms. G Gayamini
Lecturer (Probationary)
Department of Computer Engineering
Faculty of Computing
General Sir John Kotelawala Defence University

MISCELLANEOUS TASKS

Proofreading

Mr.Kithsiri Amarathunga
Dean/ Senior Lecturer I
Faculty of Management, Social Sciences and Humanities
General Sir John Kotelawala Defence University

Maj.Wimansha Abeywickrama
Head of the Department
Department of Languages
Faculty of Management, Social Sciences and Humanities
General Sir John Kotelawala Defence University

Ms.P Wijeyrathna
Lecturer
Faculty of Management, Social Sciences and Humanities
General Sir John Kotelawala Defence University

Graphic Designing

Mr. Gagana Abeyrathna
Undergraduate student
Department of IT
General Sir John Kotelawala Defence University

IT Support

Centre for IT Support and Development Services
General Sir John Kotelawala Defence University

Contents

Date of publication July 31, 2022, date of current version Aug. 12, 2022.

SQL Injection Detection and Preventive Approach for Web Applications

GJM Ariyathilake1 [1#], MHR Sandeepanie [2] ,and PL Rupasinghe [3]

[1],

Centre for Defence Research and Development, Ministry of Defence, Sri Lanka, [2]General Sir John Kotelawala Defence University, Sri Lanka,

[3]Sri Lanka Institute of Information Technology, Sri Lanka
[1#]awert1232003@gmail.com

ABSTRACT Presently, the most highly used method of global communication is web applications and used for long-distance communication, online marketing, research and development, distance learning, e-banking and social media networks. Since web applications are available for the global community with access for anyone, web applications confront numerous security issues, specifically due to web-based c yber-attacks. The SQL injection attack is the most prevailing web-based cyber-attacks globally, belonging to high-rank classifications. Because of the increased number of global online services with a high rate, SQL injection attacks also are amplified r apidly. Most SQL injection attacks are successful due to a lack of proper validation. However, a successful SQL injection attack highly interferes with databases' integrity, availability, and confidentiality. Therefore, there is a vital global requirement to overcome SQL injection attacks. Accordingly, there are three key objectives. The first objective is to detect the SQL injection attacks affecting web servers. The second objective is to explore the preventive solution for SQL injection attacks affecting the web servers. The third objective is to share the knowledge on SQL injection attacks with other researchers. Towards overcoming predominant issues, a periodically and continuously running PHP-based programme, which can identify patterns of SQL injection attacks recorded in PHP Apache log files and blocking the identified suspicious IP addresses, was designed as the adopted me thodology. Statistics of total suspicious IP addresses and black listed IP addresses with their hitting counts and time were obtained while preventing access of black listed IP addresses to the Apache webserver. The proposed solution facilitates continuous monitoring of suspicious activities while blocking vulnerable hosts using its IP addresses automatically with securing web servers from the SQL injection attack.

INDEX TERMS: Cyber-attacks, Global Communication, SQL injection attacks, Web applications.

I INTRODUCTION

The most highly used method of global communication is web applications. Web applications are used globally for long-distance communication, online marketing, health services, research and development, distance learning, e-banking and social media networks. Ever since the web applications are accessible for the global community with having access for anyone at any time, web applications have been confronted with numerous challenges comprising the security issues, precisely owing to web-based cyber-attacks. Among various cyber-attacks, the Structured Query Language (SQL) injection attack is the most prevailing web-based cyber-attacks globally, belonging to high-rank classifications. In view of that, the line of codes describe the basic SQL injection attack as follows: The statement = "select * from customers where name = '" + customerName + "';"

Above mentioned SQL code is created to pull up all the user records specified "customer name" from its table of "customers". Conversely, if the "customerName" variable is crafted and explicitly designed by one of the vulnerable users, the SQL statements may perform more than the author intended. For instance, setting the "customerName" variable using as follows:
' OR '1'='1

Alternatively, consuming comments even to block the rest of statements of the query (In here, mentioned three types of different SQL comments). All the lines have a specified space at the end of each of three statements as follows:

i. 'OR '1'='1' –
ii. ' OR '1'='1'
iii. ' OR '1'='1' /*

The above codes render one of the above mentioned SQL statements by parent language as follows:
i. select * from customers where name = '' or '1'='1';
ii. select * from customers where name = '' or '1'='1' – ';

When these codes are to be consumed in an authentication role procedure, then the above example could be utilised to force to get a selection of every field of data (*) from a customer SQL table, excluding one specified customer name, as the author intended, due to the evaluation of code '1'='1' usually is always true. The above value of

”customerName” in the statement mentioned below would cause the deletion of the ”customers” table (SQL) as well as get a selection of all the data from the ”customerinfo” table (in essence that revealing the information regarding every user), using user API that allows more SQL statements:

```
a’;DROP TABLE customers; SELECT * FROM customer-
info WHERE ’t’ = ’t
```

Such input renders the executing final SQL statements as follows:

```
select * from customers where name = ’a’;drop table
customers;
select * from customerinfo where ’t’ = ’t’;
```

To prevent SQL injection cyber-attacks, web application developers may use specific tools to check the availability and prevention of SQL injection attacks. At present, such tools are WAF (Web Application Firewall) , “Positive Tainting”, “SQLrand”, “CSSE”, “CANDID” etc.

Nevertheless, web application security is extremely vital in preventing SQL injection attacks. The developers are subjected to numerous cyber-attacks because of improper security coding practices, particularly malicious source code injection. Further, several improper and insecure coding practices are frequently used with low encryption, which is subjected to a lack of protection. Typically, SQL injection cyber-attacks execute through inserting malicious code into a SQL query. Such malicious codes, which the cyber attackers insert, are pretended as legitimate SQL query statements. Hence, the web servers’ sequential execution of such malicious codes affects the internal system and database management systems, leading to SQL injection cyber-attacks to execute improper SQL commands. Most SQL injection attacks are effective due to a deficiency of proper validation. A successful SQL injection attack vastly interferes with the databases’ integrity, availability, and confidentiality. In addition, based on the research findings and general statistics and the available data on the internet, such SQL injection cyber-attacks have a severe impact on global organisations. Accordingly, a practical solution is a vital global requirement to overcome SQL injection attacks. With this view, there are three key objectives in this research. The first objective is to detect the SQL injection attacks that affect the web servers. Afterwards, the second objective is to explore the preventive solution for SQL injection attacks affecting the web servers. Finally, the third objective is to share the knowledge on SQL injection attacks with other researchers.

II LITERATURE REVIEW

At present, most people use web applications, which are accessed through World Wide Web, precisely for long distance communications, online marketing, distance learning, e-banking and social media networks. Most of the web applications are available for anyone globally without any restrictions. Because of such reasons, it is exposed to many challenges comprising more security issues cum cyber-attacks via the internet. Consequently, Lijiu (2010) revealed about the web application vulnerabilities, such as malicious file execution, cross site scripting, SQL injection and cross site request forgery, which have the connection with secure coding of web applications. Further, Mark (2006) also studied web application security vulnerabilities, including different analysis tools. Moreover, Mark (2006) identified different analysis tools such as source code analysers, Black box scanners, DB scanners, Binary analysis tools, Runtime analysis tools, Configuration analysis tools and Proxy analysis tools. Accordingly, the ”MUSIC” tool checks the mutants in the SQL source code queries. Further, the tool termed ”SUSHI” is used to resolve existing constraints in the strings. Moreover, another tool termed ”Ardilla” is used to create SQL injection attacks and test web scenarios. In addition, the tool termed ”String Analyser” is used to analyse the web strings.

In the prevailing literature, the usage of web applications with validation using cryptographic modules and increasing cyber threats related to security of web applications have been explored (Dima, 1999). In view of that, web applications are able to use the modules for password cryptography, password generating and so on (Dima, 1999). Further, Dima (1999) explored the usages connected to web application components and how they are developed overcoming the increasing cyber threats. Further, the usages related to firewalls as a way of network site protection against external intrusions and attacks were also explored in the prevailing literature. In addition, Dima (1999) explored the different components in a firewall policy such as filtering packets, proper authentication, and application gateways. Web based cyber-attacks occur as SQL injection attacks and they prevail globally and cause severe impacts with web applications. SQL injection attacks are conducted with including a segment of malicious code into SQL query via none or without proper validated environment and that will receive by web servers. It was found that there are faults regarding web applications; the most hazardous types of vulnerabilities are Cross site scripting and SQL injection attacks (Jose, 2008). It was identified the different types of issues related to web application cyber-attacks such as injection of commands, traversal of path, LDAP injection, SQL injection and Spoofing of content (Sven, 2008). Further, more critical vulnerabilities are occurred due to cross site scripting and SQL injection attacks (Jose, 2008). Moreover, Lijiu (2010) revealed that web application vulnerabilities such as malicious file execution, cross site scripting, SQL injection and cross site request forgery connect with secure coding of web applications. It was explained regarding the vulnerabilities of SQL injection attacks & cross site scripting, which caused harm to several web applications (Andrea, 2012). There are several SQL injection detection, and prevention tools are available. Some are IDPs, Green SQL, dotDefender, Code scan labs Etc. A mole is an open-source tool for detecting SQL injection attacks. It generates reports regarding SQL injection attacks. It evaluates provided URL of clients (Pavitra Shankdhar, 2021).

Green SQL is an open-source application for detecting and preventing SQL injection attacks. It supports "My SQL" databases and evaluates SQL commands with a risk scoring matrix. It generates reports regarding the SQL injection attacks and blocks the vulnerable hosts(Ivano Alessandro Elia, 2010).

SQLsus is an open source tool for detection of SQL injection attacks. This tool can use for MySQL data bases. It is written with "PERL" computer language. This tool is fast and effiecient with detection of SQL injection attacks(Ivano Alessandro Elia, 2010). SQLMap is an open source automatic SQL injection attacks and database take over application which is used for penetration testing. This tool automates detection and exploitation of SQLi flaws.(Drew Robb, 2022) Several researchers have introduced different SQL detection and preventive solutions based on the prevailing literature. Accordingly, Rai and Nagpal (2019) studied SQL injection attacks and proposed methods and tools for detection and preventive solutions while discussion their effectiveness. Further, Singh et al. (2014) also proposed a model to block the SQL injections while analysing the existing detection prevention techniques against SQL injection attacks. Moreover, Jemal et al. (2020) also proposed solutions to mitigate SQL injection, specifically through ontology and machine learning. A differential process to safeguard against SQL injection attacks, used in ASP.NET apps, has been introduced (Kausar et al., 2019). In addition, Hu (2017) introduced a defence resistance and remedy model of SQL injection attack, established from non-intrusive SQL injection attack and defence.

III METHODOLOGY AND EXPERIMENTAL DESIGN

In achieving the study's objectives, the methodology adopted by the researchers was creating an environmental variable for the "php.exe" file as the first step. As the second step, a "bat" file for run "sql_injection_block.php" file was created. As the third step, a "task scheduler" adding "bat" file to run the "sql_injection_block.php" file continuously with appropriate time intervals was created. APACHE log files to the proposed application with the given command prompt command were linked as the final step. The adopted SQL injection attack identification and IP address blocking process are descriptively displayed (Figure 1).

Accordingly, when the user input malicious code for SQL injection attack, it will compare with SQL injection attack patterns and if the user input compares with specified patterns, then the user input attempt will take as a suspicious attempt. If the number of attempts exceeded more than the specified number of attempts, then that host IP address will be blocked automatically. All the suspicious attempts will be stored in the "suspicious_ips" file. Blocked IPs are too added to another file called "blocked_ips".

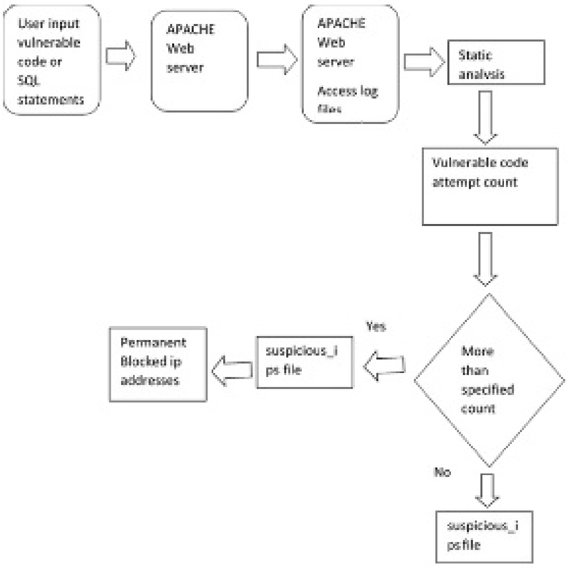

User input vulnerable code or SQL statements
APACHE Web server
APACHE Web server Access log files
Static analysis
Vulnerable code attempt count
More than specified count
Yes
suspicious_i ps file
Permanent Blocked ip addresses
No
suspicious_i ps file

Figure 1. SQL Injection attack identification and IP address blocking process
Source: Developed by the researchers based on the research study

The proposed solution has removal facility of blocked IP addresses from the blacklisted list. User input time will also be stored in the "suspicious_ips" file, and it will be able to analyse later.

A Access Log Analysis Methodology

First, have to set the path to APACHE access log files in the "apache_acess.bat" file. Then it has to connect to the task scheduler, and it is required to set the interval of time that want to run reiterately. Source code files have been located and it is required to give path of the "sql_injection_block.php" with suitable parameters in the bat file. All the installation and operatable processes will be mentioned later in a detailed manner. After installation, Apache access log files will be analysed after a specified period in the task scheduler, and all the suspicious user attempts in the apache log files will be stored in the "suspicious_ips". If there are a considerable number of suspicious attempts made by a user, then the IP is automatically blocked after exceeding previously defined value and added to the "blocked_ips" list. If it is required to remove some identified blocked IP from the blocked IP list, it will remove such IP from the blocked IP list. Such operations are mentioned in a detailed manner later. POST or GET user inputs will be analysed, and therefore any POST or GET malicious user inputs will be blocked with this solution.

B Specified SQL Injection Comparing Patterns

```
apacheaccesspaterns[] = ”/|select[\*]from|select \* from|select\*from|’or’1’=1|/i”
apacheaccesspaterns[] = ”/or1=1|update set|insert into|delete from|/i”
apacheaccesspaterns[] = ”/order by|1’1|select count([\*])|1 and 1=1|/i”
apacheaccesspaterns[] =”/&#49|&#32|&#79|&#82|&#61|&#39|1 UNION ALL SELECT 1,2,3,4,5,6,name FROM sysObjects WHERE xtype = ’U’ –|/i”
```

C Installation Process for Manual Process

This solution was designed for Windows Operating System, but later, the research will continue for Linux Operating System. This solution was designed with "XAMPP" installer. At first, it is required to install "XAMPP" software. Then it is required to set environmental variable path to PHP folder as follows; First, go to the control panel.

- First, go to the control panel.
- Then, go to “system”.
- Next, go to “change setting”.
- Then, go to “Advanced” tab.
- Then, go to environmental variables.
- Then, select the "Path" environmental variable (Figure 2) and go to "Edit", and click.
- Then, click new and type or copy and paste the path to the "PHP" folder (Figure), select the area and click the "ok" button.

Afterwards, it is required to locate the "sql_injection_block" folder as your preference. Then, it is required to open a command prompt and change the command prompt location to the "sql_injection_block" directory.

D Manual Operating Process

At first, it is required to take the command prompt location to “sql_injection_block” directory location and enter the command, “php sql_injection_block.php”, “php sql_injection_block.php -h” or “php sql_injection_block.php –help”.

Obtaining user operating options and details option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php
```

Obtaining user operating options and details option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -h
```

Obtaining user operating options and details option 3

```
C:\xampp\htdocs\sql_injection_block> php
sql_injection_block.php –help
```

1 Obtaining Statistics:

Firstly, it is required to take the command prompt location to “sql_injection_block” directory location and enter the command,
“php sql_injection_block.php –statistics” or
“php sql_injection_block.php -s”.

Obtaining statistics option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -s
```

Obtaining statistics option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –statistics
```

When entering the above mentioned command for the first time, it will be appeared as "No data!" due to the absence of the "suspicious_ips" file. Before obtaining the statistics it is required to parse the apache log files as below figure entering command "PHP sql_injection_block.php –parse-apache-log –path=C:\xampp\apache\logs\access.log".

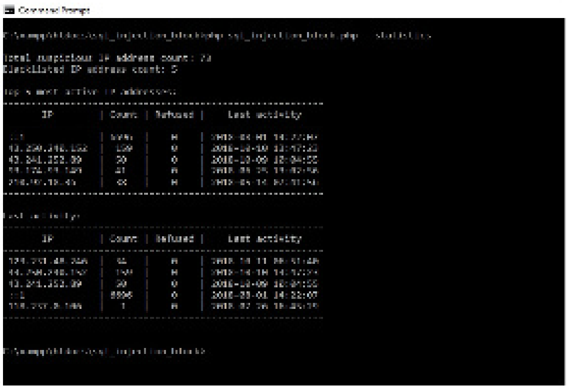
Initially, it is required to take the command prompt location to “sql_injection_block” directory location and enter the command,
“php sql_injection_block.php –parse-apache-log –path=C:\xampp\apache\logs\access.log”.

Parsing APACHE log files option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –parse-apache-log –
path=C:\xampp\apache\logs\access.log
```

Parsing APACHE log files option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -a -C:\xampp\ apache\
logs\access.log
```



```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --statistics

Total suspicious IP address count: 73
Blacklisted IP address count: 5

Top 5 most active IP addresses:
----------------------------------------------------------
      IP          | Count | Refused |    Last activity

 ::1              | [illegible] |    0    | [illegible]
 43.250.240.152   |  159  |    0    | 2018-10-10 11:47:22
 43.241.252.89    |   30  |    0    | 2018-10-09 12:04:55
 [illegible]      |   41  |    0    | [illegible]
 [illegible]      |   [illegible]  |    0    | [illegible]
----------------------------------------------------------

Last activity:
----------------------------------------------------------
      IP          | Count | Refused |    Last activity
----------------------------------------------------------
 123.231.48.246   |  [illegible]  |    0    | [illegible]
 43.250.240.152   |  159  |    0    | [illegible]
 43.241.252.89    |   30  |    0    | 2018-10-09 12:04:55
 ::1              | 5996  |    0    | 2018-03-01 14:22:07
 [illegible]      |    1  |    0    | [illegible]
----------------------------------------------------------


C:\xampp\htdocs\sql_injection_block>
```

Figure 2. Obtaining statistics
Source: Developed by the researchers based on the research study

Firstly, it is required to take the command prompt location to ”sql_injection_block” directory location and enter the command, ”PHP sql_injection_block.php –statistics” or”PHP sql_injection_block.php -s”.

Obtaining statistics option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -s
```

Obtaining statistics option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –statistics
```

After parsing APACHE access log files, it is possible to obtain the statistics (Figure 5).

2 *Obtaining List of Black Listed IP Addresses:*

Initially, it is required to take the command prompt location to ”sql_injection_block” directory location and enter the command, ”PHP sql-injection-block.php –list” or”PHP sql_injection_block.php -l”.

Obtaining black listed IP addresses option 1

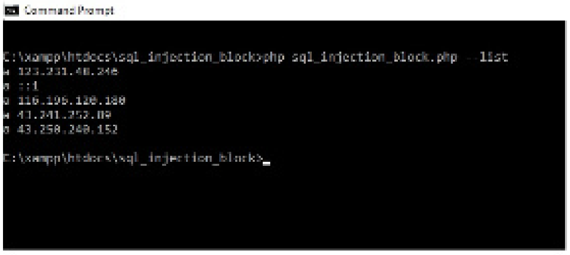
```
C:\xampp\htdocs\sql_injection_block>
php sql-injection-block.php -l
```

Obtaining black listed IP addresses option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –list
```

When entering the above mentioned command for the first time, it is appeared as ”No data!” due to absence of the ”suspicious_ips” file. Before obtaining statistics, it is required to parse the apache log files as in below (Figure 3) entering command ”PHP sql_injection_block.php –parse-apache-log –path=C:\xampp\apache\logs\access.log”.

Firstly, it is required to take the command prompt location to “sql_injection_block” directory location and enter the command, “php sql_injection_block.php –parse-apache-log –path=C:\xampp\apache\logs\access.log”. –path=C:\xampp\apache\logs\access .log”.



```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --list
# 123.231.48.246
# ::1
# 116.196.120.180
# 43.241.252.89
# 43.250.240.152

C:\xampp\htdocs\sql_injection_block>_
```

Figure 3. Obtaining blacklisted IP addresses
Source: Developed by the researchers based on the research study

Firstly, it is required to take the command prompt location to ”sql_injection_block” directory location and enter the command, ”PHP sql_injection_block.php –list” or”PHP sql_injection_block.php -l”.

Obtaining black listed IP addresses option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -l
```

Obtaining black listed IP addresses option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php–list
```

After parsing APACHE access log files, it is possible to get blacklisted IP addresses.

3 *Obtaining List of Black Listed IP Addresses with Suspicious Activity Count:*

Firstly, it is required to take the command prompt location to ”sql_injection_block” directory location and enter the command,”PHP sql_injection_block.php–list –count” or”PHP sql_injection_block.php -l -c”.

Obtaining black listed IP addresses with suspicious count option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -l -c
```

Obtaining black listed IP addresses with suspicious count option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php–list –count
```

When entering the above mentioned command for the first time, it is appeared as ”No data!” due to absence of the ”suspicious_ips” file. Before obtaining statistics it is required to parse the apache log files as below figure entering command ”PHP sql_injection_block.php –parse-apache-log –path=C:\xampp\apache\logs\access.log”.

4 *Obtaining Black Listed IPs with Suspicious Activity Time:*

Initially, it is required to take the command prompt location to ”sql_injection_block” directory location and enter the command ”PHP sql_injection_block.php –list –time” or”php sql_injection_block.php -l -t”.

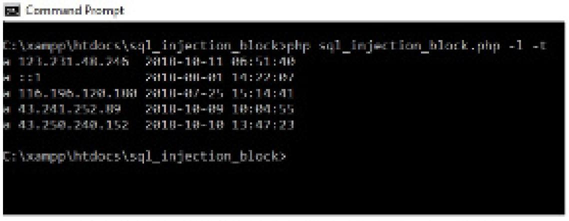
Obtaining black listed IPs with suspicious activity time option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -l -t
```

Obtaining black listed IPs with suspicious activity time option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –list –time
```

When enter the first time above mentioned command, then will get ”No data!” due to absence of the ”suspicious_ips” file. Before obtaining statistics, have to parse the apache log files as below figure entering command ”PHPsql_injection_block.php–parse-apache-log–path=C:\xampp\apache\logs\access.log”.



Command Prompt

```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php -l -t
# 123.231.48.246  2018-10-11 06:51:40
# ::1             2018-08-01 14:22:07
# 116.196.120.100 2018-07-25 15:14:41
# 43.241.252.89   2018-10-09 10:04:55
# 43.250.240.152  2018-10-10 13:47:23

C:\xampp\htdocs\sql_injection_block>
```

Figure 4. Blacklisted IPs with last activity time
Source: Developed by the researchers based on the research study

5 *Obtaining Black Listed IPs with Suspicious Activity Count and Time:*

Initially, it is required to take the command prompt location to ”sql_injection_block” directory location and enter the command, ”PHP sql_injection_block.php –list –count –time” or”php sql_injection_block.php -l -c -t”.

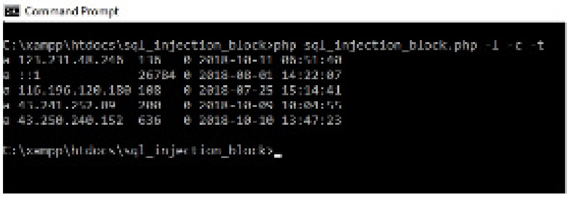
Obtaining black listed IPs with suspicious activity count and time option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -l -c -t
```

Obtaining black listed IPs with suspicious activity count and time option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –list –count –time
```

When entering the above mentioned command for the first time, it is appeared as ”No data!” due to absence of the ”suspicious_ips” file. Before obtaining statistics, have to parse the apache log files as below figure entering command ”PHP sql_injection_block.php –parse-apache-log –path=C:\xampp\apache\logs\access.log”.



Command Prompt

```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php -l -c -t
# 123.231.48.246  116   0 2018-10-11 06:51:40
# ::1             26784 0 2018-08-01 14:22:07
# 116.196.120.100 108   0 2018-07-25 15:14:41
# 43.241.252.89   208   0 2018-10-09 10:04:55
# 43.250.240.152  636   0 2018-10-10 13:47:23

C:\xampp\htdocs\sql_injection_block>_
```

Figure 5. Parsing APACHE access log files obtaining blacklisted IPs with suspicious activity count and time
Source: Developed by the researchers based on the research study

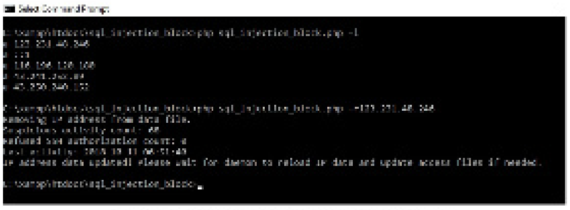
6 *Removing Black Listed IP Addresses and Adding to White List:*

Removing black listed IP option 1

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php -r123.231.48.246
```

Removing black listed IP option 2

```
C:\xampp\htdocs\sql_injection_block>
php sql_injection_block.php –
romove=123.231.48.246
```



Select Command Prompt

```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php -l
# 123.231.48.246
# ::1
# 116.196.120.100
# 43.241.252.89
# 43.250.240.152

C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php -r123.231.48.246
Removing IP address from data file.
Suspicious activity count: 48
Refused SSH authorization count: 0
Last activity: 2018-10-11 06:51:40
IP address data updated! Please wait for daemon to reload IP data and update access files if needed.

C:\xampp\htdocs\sql_injection_block>_
```

Figure 6. Removing blacklisted IPs
Source: Developed by the researchers based on the research study

E *Installation Process for Automated Process*

This solution was designed for Windows Operating System and later research will be continued for Linux Operating System. This solution was designed with ”XAMPP” installer and. At first, it is required to install “XAMPP” software.

1 *Setting the Environmental Variable Path to PHP Folder:*

Setting the environmental variable path to PHP folder as follows;

1. First, go to the control panel.
2. Then, go to "system".
3. Next, go to "change setting".
4. Then, go to "Advanced" tab.
5. Then, go to environmental variables.

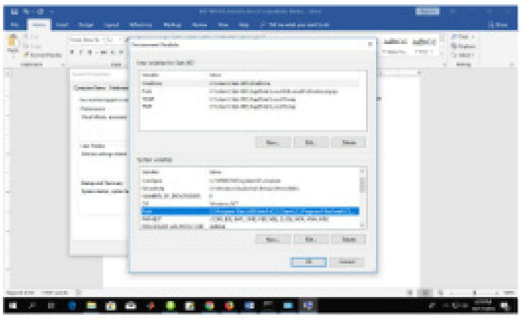
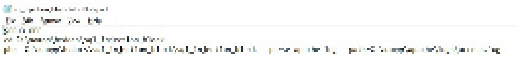


Figure 7. Environmental variables
Source: Developed by the researchers based on the research study

6. Then, select the "Path" environmental variable as in the above "Figure 10" and go to "Edit" and click.
7. Then, click new and type or copy and paste the path to the "PHP" folder as in the below figure, selected area and click the "ok" button.
8. Create the "sql_injection_block.bat" file as in below (Figure 8).



```
[illegible]
cd C:\xampp\htdocs\sql_injection_block
php C:\xampp\htdocs\sql_injection_block\sql_injection_block.php [illegible] C:\xampp\apache\logs\access.log
```

Figure 8. sql_injection_block.bat file
Source: Developed by the researchers based on the research study

In here, "cd <sql_injection_block directory path> "PHP <path to the apache access log file>" are inserted.

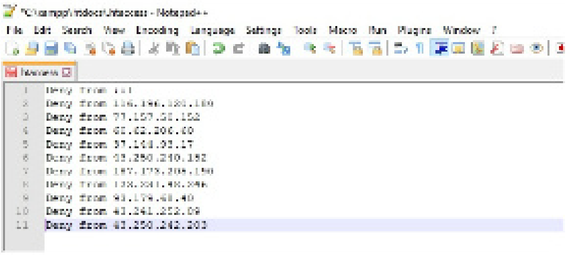
9. Then locate the "sql_injection_block.bat" file in the sql_injection_block directory.

2 *Adding the Bat File to the "Task Scheduler":*

1. Go to the start menu and type "control panel" and click it.
2. Then, go to "Administrative tools".
3. Then, go to "Task schedular".
4. Create new task"sql_injection_block". It is required to set triggering settings for at least thirty minutes and repeat activity after every thirty minutes and it is required to make sure not to set run multiple processes. Then, it is required to set settings as Queue.
5. Then run the task "sql_injection_block".

F *IP Addresses Blocking Process*

After the vulnerable IP addresses are detected, the identified IP addresses will be added to the "suspicious_ips" file. Then, that suspicious IP address will be added to the ".htaccess" file for access denied. When it is required to remove a blocked IP address, then the IP address will be removed from the ".htaccess" file.



*C:\xampp\htdocs\.htaccess - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
.htaccess

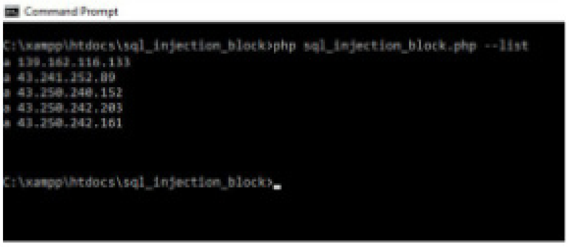
```
Deny from ::1
Deny from 116.196.120.180
Deny from 77.157.50.152
Deny from 61.62.206.60
Deny from 37.148.93.17
Deny from 43.250.240.182
Deny from 187.175.205.150
Deny from 132.241.48.246
Deny from 91.179.68.40
Deny from 43.241.252.09
Deny from 43.250.242.203
```

Figure 9. htaccess file inside
Source: Developed by the researchers based on the research study

G *Performance Analysis and Evaluation of the Current System*

When the user requests and inputs malicious codes or any input that caused to SQL injection attack or any valid user purposes, it will be compared with SQL injection primitive attack patterns and then user requests and inputs will be compared with specified patterns in the proposed system. As well as, if such user requests are matched with specified malicious patterns in the proposed system, such user input attempts will be taken as suspicious attempts, and the IP address of such attempts coming will be taken as the suspicious IP address. If several such attempts are exceeded more than a specified number of malicious attempts, then that host IP address will be blocked automatically. All the suspicious attempts will be stored in the "suspicious_ips" file. Blocked IPs added to another file called "blocked_ips". If it is required to remove the blocked IP address from the list, this solution has a facility to do that. It was explained earlier. User input times will also be stored in the "suspicious_ips" file, which will be able to analyse later.

As the first step, it is required to set the path to APACHE access log files in the "apache_acess.bat" file. Then it is required to connect to the task scheduler, and it is required to set the interval of time that want to run reiterately. Source code files have to be located and it is required to give path of the "sql_injection_block.php" with suitable parameters in the bat file. All the installation and operatable processes will be mentioned later in a detailed manner. After installing the Apache access log files, it will be analysed after the specified period in the task scheduler, and all the suspicious user attempts in the apache log files will be stored in the "suspicious_ips". If user suspicious attempts are more than the specified count of the source code, then that user will be blocked automatically and added to the "blocked_ips" list. If it is required to remove some identified blocked IP from the blocked IP list, it will remove such IP from the blocked IP list. Such operations were mentioned in a detailed manner earlier with commands. POST or GET user inputs will be analysed, and therefore any POST or GET malicious user inputs will be blocked with this solution. After processing of the "suspicious_ips" file, if suspicious pattern, matching count is exceeded the specified count in the proposed system, then such IP addresses will be added to the ".htaccess" file as "deny access ¡IP address¿". Then that IP address will be blocked for external users for internet access.



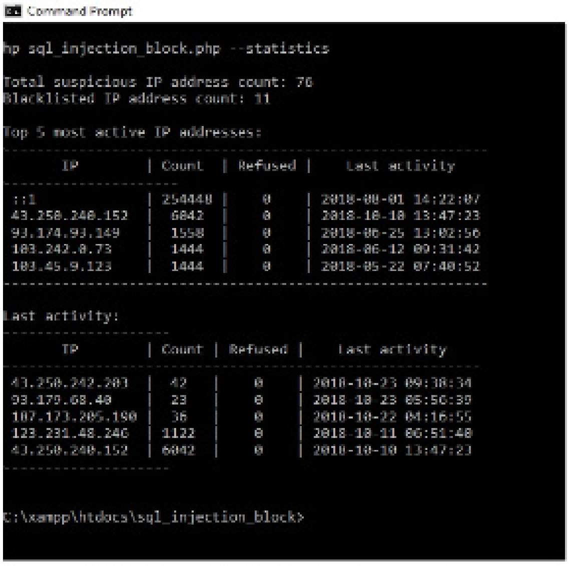
```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --list
a 139.162.116.133
a 43.241.252.89
a 43.250.240.152
a 43.250.242.203
a 43.250.242.161


C:\xampp\htdocs\sql_injection_block>_
```

Figure 10. Blacklisted IP addresses
Source: Developed by the researchers based on the research study

The detailed results are descriptively elaborated under the section of Results.

IV RESULTS

Under this section, the statistics of the user requests are explained. The result issuing command, namely, "—statistics", the most active top five addresses termed 127.0.0.1, 43.250.240.152, 93.174.93.149, 103.242.0.73 and 103.45.9.123 were obtained. The recorded occurrence of the IP address of 127.0.0.1 was 254448. The recorded occurrence of the IP address of 43.250.240.152 was 6042. The recorded occurrence of the IP address of 93.174.93.149 was 1558. The recorded occurrence of the IP address of 103.242.0.73 was 1444. The recorded occurrence of the IP address of 103.45.9.123 was 1444.



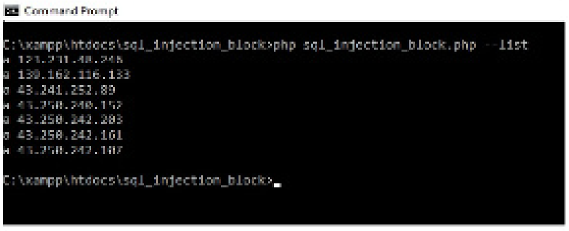
```
hp sql_injection_block.php --statistics

Total suspicious IP address count: 76
Blacklisted IP address count: 11

Top 5 most active IP addresses:
-----------------------------------------------------------------
       IP          | Count  | Refused |      Last activity
---------------------
  ::1              | 254448 |    0    | 2018-08-01 14:22:07
 43.250.240.152    |  6042  |    0    | 2018-10-10 13:47:23
 93.174.93.149     |  1558  |    0    | 2018-06-25 13:02:56
 103.242.0.73      |  1444  |    0    | 2018-06-12 09:31:42
 103.45.9.123      |  1444  |    0    | 2018-05-22 07:40:52
-----------------------------------------------------------------

Last activity:
---------------------
       IP          | Count | Refused |      Last activity
----------------------------------------------------------------
 43.250.242.203    |  42   |    0    | 2018-10-23 09:38:34
 93.179.68.40      |  23   |    0    | 2018 10 23 05:56:39
 107.173.205.190   |  36   |    0    | 2018-10-22 04:16:55
 123.231.48.246    | 1122  |    0    | 2018 10 11 06:51:40
 43.250.240.152    | 6042  |    0    | 2018-10-10 13:47:23
---------------------


C:\xampp\htdocs\sql_injection_block>
```

Figure 11. Analysed user request statistics
Source: Developed by the researchers based on the research study

The analysed and processed statistics of user requests, which the users requested, are descriptively displayed (Figure 11). The counted malicious attempts and the top five IP addresses are descriptively displayed in Figure 12. Further, the last activity time figures also are displayed. The last activity recorded date and time for IP address 127.0.0.1 was 2018-08-01 at 14:22:07. The last activity recorded date and time for IP address 43.250.240 was 2018-10-10 at 13:47:23. The last activity recorded date and time for IP address 93.174.93.149 was 2018-06-25 at 13:02:56. The last activity recorded date and time for IP address 103.242.0.73 was 2018-06-12 at 09:31:42. The last activity recorded date and time for IP address 103.45.9.123 was 2018-05-22 at 07:40:52. According to the second table of Figure 16, the last five IP addresses with the last activity details are displayed.

A Listing of Black Listed IP Addresses

According to figure 16, they were obtained using the "–list" command in the console. IP address blacklist happened due to the host trying for vulnerable patterns as HTTP requests several times. After exceeding the predefined maximum count, IP addresses were blacklisted as vulnerable IP addresses. The results of the listing of blacklisted IP addresses is descriptively displayed.



Command Prompt

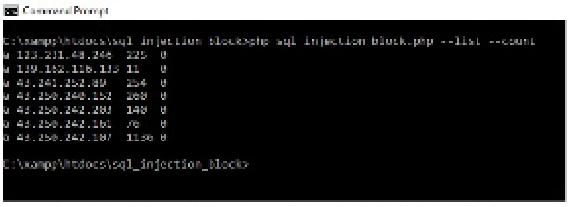
```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --list
@ 123.231.48.246
@ 139.162.116.133
@ 43.241.252.89
@ 43.250.240.152
@ 43.250.242.203
@ 43.250.242.161
@ 43.250.242.107

C:\xampp\htdocs\sql_injection_block>
```

Figure 12. Listing of blacklisted IP addresses
Source: Developed by the researchers based on the research study

The above mentioned "Listing of blacklisted IP addresses". Listing of blacklisted IP addresses that user requests are coming from. The IP addresses mentioned in "Figure 11" shows requested vulnerable requests more than the specified vulnerable attempt count in the proposed solution. After entry of the statement termed, "Deny from <IP address>" to the ".htaccess" file, accessing the webserver was blocked for that specific IP address. "403 forbidden" Error occurred after that host tried to access again. The blacklisted IP addresses are 123.231.48.246, 139.162.116.133, 43.241.252.89, 43.250.240.152, 43.250.242.203 43.250.242.161, and 43.250.242.107 were received after analysing of apache access.log file. If it is required to remove some IP addresses from the blacklisted list, then it will not appear in the blacklisted IP address list and that IP address will be able to access the webserver continuously without any hindrance. Then, IP details of the "suspicious_IPs" file will be updated stored in the "suspicious_IPs" file. "–remove = < IP address >" command used to remove IP address from the blacklisted IP address list. After analysing apache access.log files, these blacklisted IP address details will be stored in the "suspicious_IPs" file and then later also could be able to analyse and will be able to get the backup copies. When using the "–list" command other details such as; blacklisted time, suspicious occurrences count, last activity time like such details regarding that IP address will not be displayed, and only the IP address will be displayed. If such details are required, then it is required to enter other commands and that commands will be explained in a detailed manner later.

B Listing of Black Listed IP Addresses with Suspicious Attempt Count

According to figure 18, the results of listing blacklisted IP addresses with a count of vulnerable activities tried as HTTP requests are descriptively shown. When using the "–list –count" command other details such as; blacklisted time, last activity time like such details regarding that IP address will not be displayed and only IP address with a count of occurrences of vulnerable activities as HTTP requests will be displayed. If such details are required, it is required to enter other commands, which will be explained later. After issuing the "–list –count" command, blacklisted IP addresses with vulnerable activity count is shown in figure 17, "5.3 listing of blacklisted IP addresses with suspicious attempt count".



Command Prompt

```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --list --count
@ 123.231.48.246  225  0
@ 139.162.116.133 11   0
@ 43.241.252.89   254  0
@ 43.250.240.152  260  0
@ 43.250.242.203  140  0
@ 43.250.242.161  76   0
@ 43.250.242.107  1136 0

C:\xampp\htdocs\sql_injection_block>
```

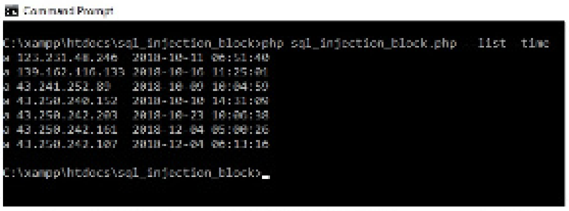
Figure 13. Listing of blacklisted IP addresses with suspicious attempt counts
Source: Developed by the researchers based on the research study

Above mentioned "Listing of blacklisted IP addresses with suspicious attempt count" provides the listing of blacklisted IP addresses that user requests with suspicious attempts count in front of them. In here 123.231.48.246, 139.162.116.133, 43.241.252.89, 43.250.240.152, 43.250.242.203, 43.250.242.161, 43.250.242.107 were the blacklisted IP addresses. The blacklisted IP address 123.231.48.246 was recorded with 225 vulnerable activity counts. The blacklisted IP address 139.162.116.133 was recorded with 11 vulnerable activity counts. The blacklisted IP address 43.241.252.89 was recorded with 254 vulnerable activity counts. The blacklisted IP address 43.250.240.152 was recorded with 260 vulnerable activity counts. The blacklisted IP address 43.250.242.203 was recorded with 140 vulnerable activity counts. The blacklisted IP address 43.250.242.161 was recorded with 76 vulnerable activity counts. The blacklisted IP address 43.250.242.107 was recorded with 1136 vulnerable activity counts. After analysing apache access.log files, these blacklisted IP address details were stored in the "suspicious_IPs" file.

There is a PHP function called "parseFile" in the Apacheaccesslogparser.php file and within that function, new IP details were added to the "suspicious_IPs" file. When issuing the command "–list –count", these details were taken from the "suspicious_IPs" file. When using the "–list –count" command other details such as; blacklisted time, last activity time like such details regarding that IP address were not displayed and only blacklisted IP addresses with vulnerable activity count were displayed. If such details are required, then it is necessary to enter other commands and that commands will be explained in a detailed manner well ahead.

C Listing of Black Listed IP Addresses with Last Suspicious Attempt Time

The results of the blacklisted IP addresses with the last activity time is displayed in figure 19. The results were obtained using the "–list –time" command in console. After analysing apache access.log files these blacklisted IP addresses and other details will be stored in the "suspicious_IPs" file, and when issuing the command "–list –time", then these details will be taken from the "suspicious_IPs" file.



Command Prompt

```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php  list  time
 123.231.48.246  2018-10-11 06:51:40
 139.162.116.133 2018-10-16 11:25:01
 43.241.252.89   2018-10-09 10:04:59
 43.250.240.152  2018-10-10 14:31:09
 43.250.242.203  2018-10-23 10:06:38
 43.250.242.161  2018-12-04 05:00:26
 43.250.242.107  2018-12-04 06:13:16

C:\xampp\htdocs\sql_injection_block>_
```

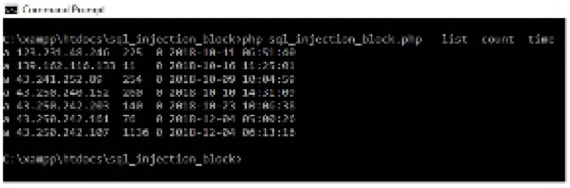
Figure 14. Listing of blacklisted IP addresses with last suspicious attempt times
Source: Developed by the researchers based on the research study

The above mentioned "Listing of black listed IP addresses with last suspicious attempt time" (Figure 14) shows the listing of black listed IP addresses that user requests coming from with their suspicious last attempted time in front of them.

In here, 123.231.48.246, 139.162.116.133, 43.241.252.89, 43.250.240.152, 43.250.242.203, 43.250.242.161, 43.250.242.107 were the blacklisted IP addresses. The blacklisted IP address 123.231.48.246 was recorded with the last vulnerable activity date and time as 2018-10-11 at 06:51:40. The blacklisted IP address 139.162.116.133 was recorded with the last vulnerable activity date and time as 2018-10-16 at 11:25:01. The blacklisted IP address 43.241.252.89 was recorded with the last vulnerable activity date and time as 2018-10-09 at 10:04:59. The blacklisted IP address 43.250.240.152 was recorded with the last vulnerable activity date and time as 2018-10-10 at 14:31:09. The blacklisted IP address 43.250.242.203 was recorded with the last vulnerable activity date and time as 2018-10-23 at 10:06:38. The blacklisted IP address 43.250.242.161 was recorded with the last vulnerable activity date and time as 2018-12-04 at 05:00:26. The blacklisted IP address 43.250.242.107 was recorded with the last vulnerable activity date and time as 2018-12-04 at 06:13:16. These details were added to the "suspicious_IPs" file from the "$ipInfo" array. The new IP details were added to the "$ipInfo" array within the "Apacheaccesslogparser.php" file. A PHP function called "parseFile" was included there and within that function, new IP details were added to the "suspicious_IPs" file.

D Listing of Black Listed IP Addresses with Suspicious Attempt Count and Last Suspicious Attempt Time

The result of listing blacklisted IP addresses with the last activity time and count of suspicious activities are shown below (Figure 15). That results were obtained using the "–list–count –time" command in console.



Command Prompt

```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php  list  count  time
 123.231.48.246  225  0 2018-10-11 06:51:40
 139.162.116.133 11   0 2018-10-16 11:25:01
 43.241.252.89   254  0 2018-10-09 10:04:59
 43.250.240.152  260  0 2018-10-10 14:31:09
 43.250.242.203  140  0 2018-10-23 10:06:38
 43.250.242.161  76   0 2018-12-04 05:00:26
 43.250.242.107  1136 0 2018-12-04 06:13:16

C:\xampp\htdocs\sql_injection_block>
```

Figure 15. Listing of blacklisted IP addresses with suspicious attempt count and last suspicious attempt time
Source: Developed by the researchers based on the research study

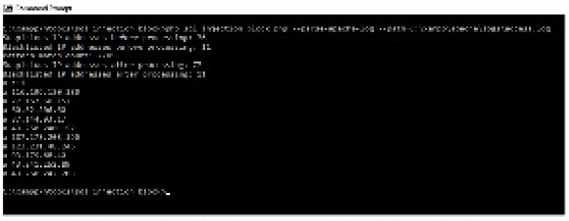
Above mentioned "Listing of blacklisted IP addresses with suspicious attempt count and last suspicious attempt time" with the listing of blacklisted IP addresses that user requests coming from with their suspicious last attempted time and suspicious attempt count in front of them. In here 123.231.48.246, 139.162.116.133, 43.241.252.89, 43.250.240.152, 43.250.242.203, 43.250.242.161, 43.250.242.107 were the blacklisted IP addresses. The blacklisted IP address 123.231.48.246 was recorded with the last vulnerable activity date and time as 2018-10-11 at 06:51:40 and the count of vulnerable activities as 225. The blacklisted IP address 139.162.116.133 was recorded with the last vulnerable activity date and time as 2018-10-16 at 11:25:01 and the count of vulnerable activities as 11.

The blacklisted IP address 43.241.252.89 was recorded with the last vulnerable activity date and time as 2018-10-09 at 10:04:59 and the count of vulnerable activities as 254. The blacklisted IP address 43.250.240.152 was recorded with the last vulnerable activity date and time as 2018-10-10 at 14:31:09 and the count of vulnerable activities as 260. The blacklisted IP address 43.250.242.203 was recorded with the last vulnerable activity date and time as 2018-10-23 at 10:06:38 and the count of vulnerable activities as 140. The blacklisted IP address 43.250.242.161 was recorded with the last vulnerable activity date and time as 2018-12-04 at 05:00:26 and the count of vulnerable activities as 76.

The blacklisted IP address 43.250.242.107 was recorded with the last vulnerable activity date and time as 2018-12-04 at 06:13:16 and the count of vulnerable activities as 1136. After analysing apache access.log files these blacklisted IP addresses and other details were stored in the "suspicious_IPs" file, and when issuing the command "–list –count –time", then these details were taken from the "suspicious_IPs" file.

E Apache Access Log File Analysis

The results of parsing Apache access.log file analysis is displayed below (Figure 16). That results were obtained using the "–parse-apache-log –path = <path to the Apache access.log file>" command in console. In here, "suspicious IP addresses before processing: 76" means, before parsing Apache access.log file for the processing which was previously stored suspicious IP addresses count in the "suspicious_IPs" file is 76. When single suspicious activity was encountered from an IP address, then that IP address was taken as a suspicious IP address. Further, it became a blacklisted IP address when exceeding the predefined suspicious activity count.



```
[illegible]
```

Figure 16. Apache access log file analysis
Source: Developed by the researchers based on the research study

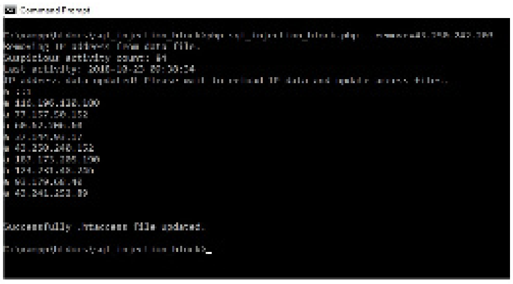
Above mentioned "Apache access log file analysis" in "Figure 16" shows the listing of blacklisted IP addresses that user requests coming from with suspicious IP addresses count before processing, Blacklisted IP addresses count before processing, Total vulnerable pattern match count, suspicious IP addresses count after processing, Blacklisted IP addresses count after processing.

Here, "Blacklisted IP addresses before processing was 11" means, before parsing Apache access.log file for processing. Previously stored blacklisted IP addresses count in the "suspicious_IPs" file is 11. Here total vulnerable pattern match count was 7785. Here "suspicious IP addresses after processing: 77" means, after parsing Apache access.log file for processing total stored suspicious IP addresses count in the "suspicious_IPs" file is 77 and new one suspicious IP address added to the "suspicious_IPs" file after parsing the Apache access.log file for processing.

Here "Blacklisted IP addresses after processing was 11" means that after parsing Apache access.log file for processing, the total stored blacklisted IP addresses count in the "suspicious_IPs" file was 11. It means no new blacklisted IP address was added to the "suspicious_IPs" file.

F Removing Blacklisted IP Address

The removal of blacklisted IP addresses is shown below (Figure 17). That results were obtained using the "–remove =<IP address>" command in console. After removing the blacklisted IP address, it was stored in the "suspicious_IPs" file.



```
[illegible]
Removing IP address from data file.
[illegible]
[illegible]
[illegible]

Successfully .htaccess file updated.

[illegible]
```

Figure 17. Removing blacklisted IP address
Source: Developed by the researchers based on the research study

Figure 17 shows removing blacklisted IP addresses and after removing that IP address, all suspicious activity count of that IP address, last activity time of that IP address. All blacklisted IP addresses are listed hereafter, removing the specified IP address. When removing some IP addresses from the blacklisted IP address list, it did not appear in the blacklisted IP address list and that IP address was able to access the webserver continuously without any hindrance. Then IP details of the "suspicious_IPs" file were updated and stored in the "suspicious_IPs" file then; later can be analysed and will be able to get backup copies. The command "–remove = < IP address > " was used to remove an IP address from the blacklisted IP address list. Removing blacklisted IP addresses will do from handling ".htaccess" file. In here, ".htacess" was used to block vulnerable hosts, adding "Deny from <ipaddress>" code inside it, and this code will be added to every vulnerable blacklisted IP address to block the server access. Then it will be given a "403 Forbidden" error to the vulnerable host preventing access to the server. After removing the blacklisted IP address from the blacklisted list, then "Deny from <ipaddress>" entry will be removed from the ".htaccess" file for the relevant removed IP address.

G Test an Evaluation of Final Host IP Address Blocking

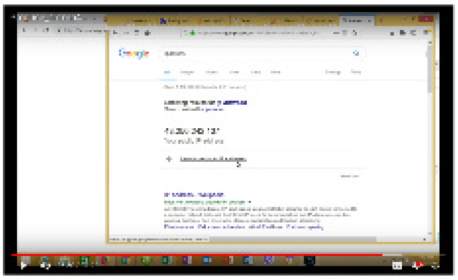
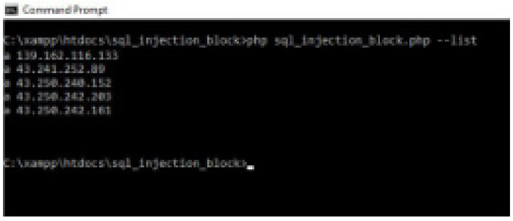


Figure 18. Host public IP address
Source: Developed by the researchers based on the research study

Above Figure 18 shows the tested vulnerable host public IP address (43.250.242.107).

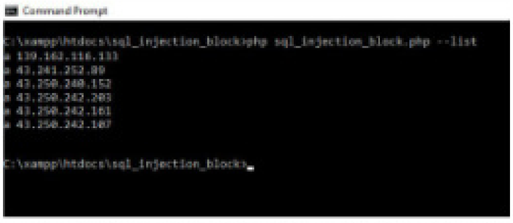


```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --list
a 139.162.116.133
a 43.241.252.89
a 43.250.240.152
a 43.250.242.203
a 43.250.242.161


C:\xampp\htdocs\sql_injection_block>_
```

Figure 19. Blacklisted IP addresses
Source: Developed by the researchers based on the research study

Above figure 15 shows the black listed vulnerable host public IP addresses. Above figure 19 shows that the public IP address (43.250.242.107) did not belong to the black listed IP addresses after removing the public IP address (43.250.242.107) from black listed IP addresses list in figure 20.

Vulnerable host (public IP address (43.250.242.107)) was trying to access a web server (public IP address (43.250.242.107)) with vulnerable user inputs "'or'1'=1" continuously and after the exceeding of maximum count of vulnerable accesses IP address, 43.250.242.107 added to the blacklisted IP address list.



```
C:\xampp\htdocs\sql_injection_block>php sql_injection_block.php --list
a 139.162.116.133
a 43.241.252.89
a 43.250.240.152
a 43.250.242.203
a 43.250.242.161
a 43.250.242.107

C:\xampp\htdocs\sql_injection_block>_
```

Figure 20. Trying to access web Server with vulnerable codes
Source: Developed by the researchers based on the research study

Above figure 20 shows the IP address, 43.250.242.107 added to the black listed IP address list.

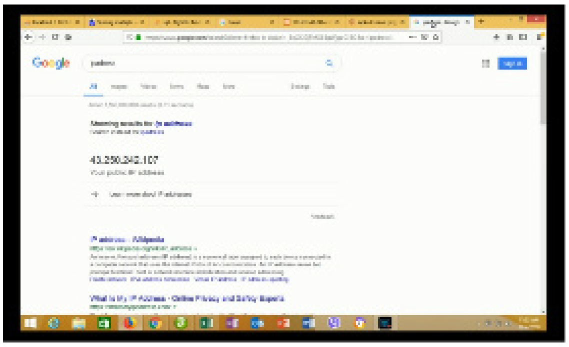


Figure 21. Trying to access web Server after vulnerable host blacklisted
Source: Developed by the researchers based on the research study

Above figure 21 shows web results when trying to access web server after vulnerable host (IP address 43.250.242.107) got blacklisted with a legitimate URL.

V DISCUSSION AND CONCLUSION

The proposed solution for SQL injection prevention facilitates the continuous monitoring of suspicious activities. Conferring to this proposed solution, there is no requirement for the user to be concerned about monitoring IP address blocking activities in web applications. Further, the proposed solution automatically blocks the vulnerable hosts using its IP address. Moreover, the proposed solution facilitates a listing of blocked IP addresses if the user needs to remove some IP addresses from the blacklisted IP address list. As well as, the user could be able to customise the blocked IP address list according to his will. Further, this proposed solution facilitates the user to view the last activity time of the suspicious IP addresses with the suspicious activity count; then, the user will compare each of the suspicious IP addresses. In view of that, all the suspicious activities will be stored in a file, including suspicious activity time and activity count; then, the user will be able to process later or analyse such details further, and such data backups are also able to take. However, the proposed solution is designed mainly for "Windows" operating systems and have to install "XAMPP" or "WAMP" software, which is freely available on the internet. The proposed solution is composed of a set of vulnerable user HTTP request patterns & it is recommended to add more vulnerable user HTTP request patterns. Then the user faithfulness to the proposed system will be increased. Further, it is recommended to use XAMPP version 7 or above. Finally, the proposed solution is recommended for "Windows 7" or above.

REFERENCES

[1] S.W. Booyd, and A.D. Keromytiss, "SQL Rand: Preventing SQL injection attacks," Colombia University, Available: https://www1.cs.columbia.edu/~angelos/Papers/sqlrand.pdf, [Accessed May 5, 2018].

[2] G. Buehrer, B. Weide, and P. Sivilotti, "Using parse tree validation to prevent SQL injection attacks," Research Gate, Available: Error! Hyperlink reference not valid. 221215947_Using_parse_tree_validation_to_prevent_SQL_injection_attacks [Accessed June 5, 2018].

[3] S. Christensen, A. Moller, and M. S. Precise, Analysis of String Expressions. Berlin, Germany: Springer, 2003, pp. 1-50.

[4] S. Faker, M. Muslim, and H. Dachlan, "A Systematic Literature Review on SQL Injection Attacks Techniques and Common Exploited Vulnerabilities," International Journal of Computer Engineering and Information Technology, vol. 9, 2017, Available: http://www.ijceit.org/ published/ volume9/ issue12/ 2Vol9No12.pdf [Accessed Jan. 26, 2018].

[5] W. Halfond, and A. Orso, Malware Detection. Boston, USA: Springer, 2007, pp. 86.

[6] E. Janot, and P. Zavarsky, "Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM," Research Gate, 2008, Available: file:///C:/Users/CRD/Downloads/2008_OWASP_AppSec_Preventing_SQL_injections_in_online_applications.pdf [Accessed Mar. 15, 2018].

[7] I. Jemal, O. Cheikhrouhou, H. Hamam, and H. Mahfoudhi, "SQL Injection Attack Detection and Prevention Techniques Using Machine Learning," International Journal of Applied Engineering Research, vol. 15, 2020, pp. 569-580.

[8] M.A. Kausar, M. Nasar, and A. Moyaid, "SQL Injection Detection and Prevention Techniques in ASP.NET Web Application," International Journal of Recent Technology and Engineering, vol. 3, 2019, pp. 7759-7766.

[9] H. Kaur and S. Dhingra, "A Review: Prevent SQL Injection Attacks Using IPS," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, 2014, pp. 8124-8126, Available: https://ijarcce.com/wp-content/uploads/2014/10/IJARCCE1I-a-amit-harpreet1-A-Review-Prevent-SQL-Injection-Attacks-Using-IPS.pdf [Accessed August 07, 2018].

[10] H. Mehta, "Threat Intelligence.," Symantec enterprise blogs security, 2018 [online] Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-patch-tuesday-november-2018 [Accessed Nov. 15, 2018].

[11] F. Mavituna, (2008). Deep Blind SQL Injection. Portcullis Security, 2008 [online] p.A11. Available: Error! Hyperlink reference not valid. / [Accessed Aug. 20, 2018].

[12] A. Makiou, Y. Begriche, and A. Serhrouchni, "Hybrid Approach to Detect SQLi Attacks and Evasion Techniques. HAL archives, 2015, Available: https://hal.archives-ouvertes.fr/hal-01138604/document [Accessed Oct. 10, 2018].

[13] R. Muhammad, S. Habib and R. Bashir, "Detection and Prevention of SQL Injection Attack by Dynamic Analyser and Testing Model," Research Gate, 2017, Available: https://www.researchgate.net/publication/319453593_Detection_and_Prevention_of_SQL_Injection_Attack_by_Dynamic_Analyzer_and_Testing_Model
[Accessed Nov. 02, 2018].

[14] S. Rai, and B. Nagpal, "Detection and Prevention of SQL Injection Attacks: Developments of the Decade," 3rd International Conference on Reliability, Infocom Technologies and Optimisation (ICRITO) (Trends and Future Directions), AIIT, Amity University Uttar Pradesh, Noida, India, 2014.

[15] J. Singh, "Analysis of SQL Injection Detection Techniques," 2017, Available: Error! Hyperlink reference not valid. 1605.02796.pdf [Accessed Jun. 08, 2018].

[16] S. Singh, U. Tripathi, and M. Mishra, "Detection and Prevention of SQL Injection AttackUsing Hashing Technique. International Journal of Modern Communication Technologies and Research (IJMCTR), [online], vol. 2, 2014, Available: https://www.academia.edu/9378445/Detection_and_Prevention_of_SQL_Injection_Attack_Using_Hashing_Technique [Accessed Aug. 22, 2018].

[17] F. Valeur, D. Mutz, and G. Vigna, "A Learning-Based Approach to the Detection of SQL Attacks," Research Gate, 2005, Available: Error! Hyperlink reference not valid. 225239186_A_Learning-Based_Approach_to_the_Detection_of_SQL_Attacks
[Accessed Jul. 15, 2018].

[18] O. Voitovych, and L. Kupershtein, "SQL injection prevention system," Research Gate, 2016, Available: https://www.researchgate.net/publication/310454603_SQL_injection_prevention_system [Accessed Aug. 15, 2018].

[19] D. Robb, "Best SQL Injection (SQLi) Detection Tools 2022," Serverwatch, 2022, Available: https://www.serverwatch. com/reviews/sql-injection-detection-tools/ [Accessed Mar. 08, 2022].

[20] P. Shankdhar, "Best free and open source SQL injection tools [updated 2021]," INFOSEC, 2021, Available: https:// resources. Infosecinstitute .com / topic / best-free – and – open – source – sql - injection-tools/ [Accessed Mar. 05, 2022].

ACKNOWLEDGMENT

We immensely thank all the professionals who supported in developing this noteworthy proposed system for SQL injection detection and prevention in various web applications. Further, we greatly thank all the researchers in the fields of Cyber Security and Software Engineering who contributed greatly to enhancing the pool of literature, which helped us in order to succeed in our creation.

AUTHOR BIOGRAPHY/IES

GJM Ariyathilake BSc(hons) in IT, MSc in IT (Specialization in Cyber Security) is working as Research Officer at Centre for Defence Research and Development

Mrs MHR Sandeepanie MBA, BSc(Special)(Hons), National Dip. Training & HRD, National Dip. HRM, IPICT(Denmark) is working as Senior Assistant Registrar at General Sir John Kotelawala Defence University and presently reading for PhD in Management at University of Sri Jayewardenepura.

Dr PL Rupasinghe PhD (Curtin University of Technology, Australia), MBA (PIM, USJ), BSc(Hons) is working as Senior Lecturer at Sri Lanka Institute of Information Technology.

Date of publication July 31, 2022, date of current version Aug. 12, 2022.

A Review on Vision-Based Obstacle Avoidance and Assistant Systems for Visually Impaired People

KLH Imesha [1#], G Gayamini [1], and B Hettige[2]

[1,2,3]1Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka.
[1#]36-ce-0009@kdu.ac.lk

ABSTRACT Travelling is one of the biggest problems faced by the visually impaired community in their day today life. Even though the visually impaired people have their own methods for travelling such as with the aid of white canes and guide dogs, those traditional methods have lot of difficulties and i ssues. Because of those i ssues, researches has paid attention to develop assistive technologies which can help the visually impaired community for their day today travelling. Although the assistant technologies are developed in the past decades, the visually impaired community faces a lot of issues when using them because of the Disability Digital Devide. As a result of this, number of systems and technologies have been introduced to the word. Those systems use different technologies like vision modules, sensors and GIS maps but most of those systems are vision-based and they use different approaches to develop their vision modules such as deep learning, reinforcement learning, stereo imaging, enhanced image processing techniques, etc. So in this paper, we will focus on those vision-based systems to find the optimal way of developing a vison-based assistant system for visually impaired people by studying those technologies and by comparing and contrasting those technologies while understanding their used modules algorithms, efficiency, usability, functionalities and their advantages and disadvantages.

INDEX TERMS: Computer Vision, Deep Learning, Smart Wearable.

I INTRODUCTION

With the help of the development of new technologies, the world is focusing on using assistive technologies to help people with disabilities to accomplish their daily tasks easier and more efficiently in work, education, communication, traveling, entertainment and other day-to-day activities. These new technologies and devices have helped to enhance the quality of the lives of differently-abled people in many ways. Among those, assistive technologies that improve the mobility of blind or visually impaired persons were given specific attention.

Vision is considered as one of the most used and powerful sensing method human have. According to World Health Organization around 220 million people worldwide have a visual impairment. Among them, 40 million are blind and 180 million have low vision.[1]

Although the new technology makes our life much easier, there is still a divide between those who are not differently-abled and those who are differently-abled to use those technologies. This gap is known as Disability Digital Divide. This gap becomes larger when it comes to visually impaired people because most of the technological devices like computers and mobile phones are vision-based operating devices. Nowadays most of the assistive technologies are widely used in smartphones but visually impaired people face different kind of problems using smartphones such as it is hard to perform specific touchscreen gestures, unawareness of supported gestures in current app, getting lost while using an app and having no way to correct it, Unable to scroll through lists, slow screen reader, lack of knowledge about the meaning of specific sounds, slow text input, changing the written text is hard, unable to find the desired option, etc.[2] Also voice commanding and audio feedbacks have issues like difficulty of recognizing audio feedback and commands in noisy surroundings, The acoustic feedbacks are not enough to give relevant information, using voice commands in public is not good for visually impaired person's privacy.[3] Even in computer and web related applications, there are usability issues for visually impaired peoples such as they cannot interact with software interfaces, can't navigate from keyboard arrow keys, screen reading software compatibility issues, etc.[4]

Because of those described problems, researchers tried to develop assistive wearable devices which is specially design to give high usability to the visually impaired people. Among this devices, navigation and travelling assistant devices take a major place because travelling is one of the major problems facing by the visually impaired community. Generally, a Vision-Based Obstacle Avoiding System has three major components named Vision Input Module, The Processing Modules and the Feedback Module.

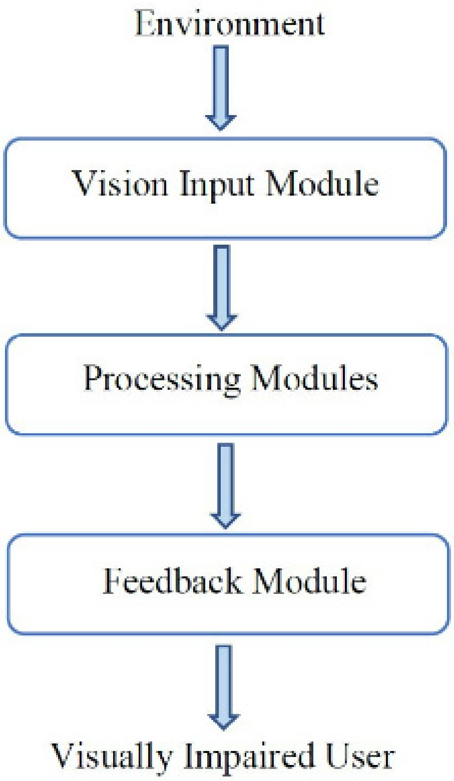


Figure 1. Flow of the process
Source: Author

he vision input module basically takes data from the environments as sequence of image frames or as sensory readings and inputs to the processing module. To take image frames as inputs, these systems use monocular cameras, stereo cameras and vision-related sensors like the Kinect sensor. For the sensory readings, most of the systems use IR sensors, Laser range finders, and Ultrasonic sensors.

Most of the time the output model is just a simple module that can give the relevant feedbacks to the visually impaired person. It generally have feedback modules like earphones and vibration modules.

The processing module can be a computer or a micro-controller which is responsible for the creation of point clouds, depth maps and the detection of edges, corners and other obstacles. This module is the most complex one in the system. Different systems use alternative methods and technologies to develop the processing module.

The designed and developed travel assistant devices use different technologies for the processing module according to their targeted functionalities. Most of the devices which were designed for indoor environments, uses short rage obstacle avoiding sensors like ultrasonic sensors, Radio-Frequency Identification (RFID) technology and models like ARIANNA (pAth Recognition for Indoor Assisted NavigatioN with Augmented perception) to identify different places, objects and paths in an indoor environment. But when analyzing the systems designed for the outdoor conditions, things get somewhat complicated. Most of these outdoor navigation systems have several modules. The main module is the vision module. Generally this module consists of a camera module. Stereo vision systems use 2 cameras (stereo cameras) and monocular vision systems use only one camera. Some of the systems also used depth sensors like Kinect sensors to identify and calculate the position of obstacles. These systems also use GPS modules to track the outdoor location and give some specific functionalities. The other main module is audio feedback module. Almost all the systems use audio feedback module because audio feedback is the easiest and the most suitable way to interact with visually impaired people. These feedbacks is mostly used to give warnings and also to give relevant instructions. In the upcoming chapter describe about those technologies and systems are described with more details to understand what are the pros and cons of those systems.

The rest of the paper organized as follows. Section II present background and related work in this field. Section III will summarize about the used technologies, algorithms and also compare and contrast them. Section IV will discuss about the conclusions we can made by comparing and analyzing different systems and section V will give the references.

II RELATED WORK

A number of researchers have studied about different technologies which is applicable to find a reliable solution to this problems facing by the visually impaired community. They have developed several systems which can give fair output using technologies like monocular and stereo vision with deep learning, reinforcement learning and other algorithms, RFID, ultrasonic technology, IR technologies, GPS, laser technologies, etc. But each of those systems have their own advantages and disadvantages in different sections like usability, reliability, speed, cost, etc. So, to get a clear idea about them it's better to review the systems developed by those different technological approaches.

A Deep Learning Approach

One of the popular technologies that used in these systems is the Deep learning approach. An interesting work done by St. Francis Institute of Technology[5] uses four-layered Convolutional Neural Network (CNN) which can scan the surroundings, detects and classifies the nearby objects as well as the distances to those relevant objects with a response time of 50ms. It also uses an ultrasonic sensor to increase the accuracy of the measured distance. This system uses audio feedback and vibrations to alert the VIPs. The work [6] provides technology with reusable way-finding with obstacle avoidance. To predict the navigation actions, they have trained a Recurrent Neural Network and for obstacle avoiding, they have fine-tuned a Convolutional Neural Network model. The paper [7] also shows how Convolutional Neural networks can be used to estimate the Transmission map for obstacle detection.

B Image Processing Techniques and Algorithms

Most of the systems use improved computer vision algorithms to Develop vision-based assistant systems for visually impaired people. The system [8] is an indoor-outdoor Navigation System specially designed for people who have low vision. This model uses ARIANNA (pAth Recognition for Indoor Assisted NavigatioN with Augmented perception) which is an indoor localization and navigations system. For outdoor conditions, it uses a computer vision system with several measurement sensors. The system has Geometry Based Path Identification which uses canny algorithms to detect path searching lines by image inputs. To improve the accuracy of those input images the system uses traditional image enhancement techniques like Gaussian smoothing and other enhancement filters to reduce noise effects. After the images convert into the canny form it can it process them to detect edges, lines and slopes. Color-Based Path identification is a functionality that make this system much better. Using this technology, the buildings like hospitals can apply color stripes on the floor and by detecting them the system can assist the visually impaired person. The system uses both the inertial sensors and the camera of the smartphone of the user as sensors

C Stereo Vision

When we consider about the systems which are using image processing techniques and algorithms, most of the researchers have paid attention for using stereo cameras because stereo cameras make it easy to calculate the depth and other details in the 3d space. The technics of these systems are mainly based on optical flow which can be described as the pattern of apparent motion of objects, surfaces, and edges in a visual picture induced by the relative motion between an observer.

The system in [9] developed in university of Alcala gives a reliable way to detect obstacles in outdoor environment and alert VIPs by audio feedbacks. As the first step, the ground plane detection is done using RANdom SAmple Consensus which is known as (RANSAC). Next the system does the Stereo Rig Calibration and Rectification to create the disparity map and calculate x, y and z coordination of obstacles. The intrinsic parameters and distortion parameters of each camera, as well as the extrinsic parameters (rotation, translation) between cameras, are estimated in the stereo rig calibration issue. Both cameras are calibrated independently and obtain the intrinsic calibration matrix for each of the cameras.

$$K = \begin{pmatrix} f_x & 0 & u_0 \\ 0 & f_y & v_0 \\ 0 & 0 & 1 \end{pmatrix}$$

Where u_0 and v_0 is the principle point of the camera and f_x and f_y are the focal lengths. The rotation matrix between cameras RLR is the identity matrix, and the translation vector TLR encodes the baseline B of the rectified stereo rig. When (u_L, u_R, v) are the stereo image projections of the same point (because in stereo images v_L = v_R = v), We can calculate X, Y and Z 3D point coordinates with respect to camera by using following equations.

$$Z = f.\frac{B}{(u_R - u_L)}$$

$$X = Z.\frac{(u_L - u_0)}{f}$$

$$Y = Z.\frac{(v - v_0)}{f}$$

After finding X, Y and Z we can find the distance and angle of the object by using the given equations.

$$Distance = \sqrt{X^2 + Z^2}$$

$$\alpha = \tan^{-1}(\frac{Z}{X})$$

After that the polar cumulative grid is projected onto it for counting about potential obstacles in the ground plane.

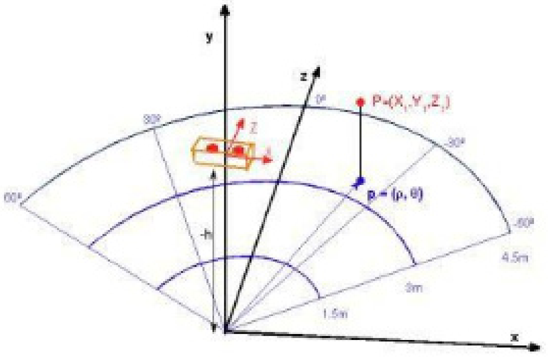


Figure 2. Creating the polar grid after calculation [10]

The system [11] also using the stereo imaging with object collision detection algorithm. It uses the disparity image or depth map as the previously discussed work[9]. That computer vision system is integrated with Blavigator prototype which is developed by University of Trás-os-Montes and Alto Douro (UTAD) known as a cheap easy to use mobile navigation system for visually impaired people providing ways to get to a given location and, while doing so, providing contextual information about obstacles and points-of-interest (POI) like zebra-crossings, building entrances by using GIS data and location data.

D Reinforcement Learning

Some researchers has tried to use monocular vision with reinforcement learning instead of stereo vision. In works like [12], they have proposed an algorithm that learns relative depth by monocular vision (only from single image) in outdoor environments. They have collected thousands of images with a laser range scan which gives the nearest obstacle in each direction of the image. Using that dataset, they trained the system with supervised learning algorithm and the system was able to accurately estimate the nearest object in the vision after the training.

E Navigation Robots

In the developed countries most of the visually impaired people use trained guide dogs in their day today travelling. Following that format, researchers have tried to develop assisting robots to guide the visually impaired people. The work like [13] and [14] uses robot assistants instead of smart wearables. These systems also has a stereo camera vision module. And they use some sensor modules like laser range finders and LiDAR in addition to the cameras to detect the obstacles. These systems use a tactical handle as the main feedback technology. It uses vibro-tactile feedback on the handle to convey directional information to the user.

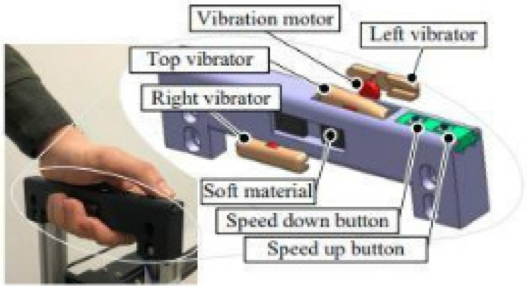


Figure 3. Modified suitcase handle with vibro-tactile feedback. [14]

F Vision and Depth Combined Sensors

When we study about the computer vision modules the most popular method is using cameras. However we can also use vision and depth combined sensors like Kinect sensor instead of cameras for special tasks like obstacle detection. Kinect sensor is Microsoft's motion sensor add-on for the Xbox 360 gaming console. It has an RGB color VGA video camera, a depth sensor, and a multi-array microphone. The camera detects the red, green, and blue color components as well as body-type and facial features.

The system [15], [16] and [17] are good examples for the systems which are using Kinect sensor and depth sensors for obstacle avoiding smart wearables. The obstacle avoiding of this system work in several steps. The point cloud registration stage seeks to create point cloud using information from the Kinect sensor like color, depth, and accelerometer data. To create the 3D point cloud from Kinect data, x, y and z coordination are calculated using this equations.

$$P3D_x = \frac{(x_c - cx_c) \times depth(x_c, y_c)}{fx_c}$$

$$P3D_y = \frac{(y_c - cy_c) \times depth(x_c, y_c)}{fy_c}$$

$$P3D_y = depth(x_c, y_c)$$

where xc and yc is the pixel coordinate in color image, cxc, cyc, f xc, f yc is taken from color intrinsic matrix, depth(xc, yc)is the depth value of pixel.

As the next step, plane segmentation is done to determine the dominant places from the point cloud by using the plane segmentation method proposed in [18] that permits real-time segmentation of point cloud data into various planes.

After processing plane segmentation step, Ground and wall detection is done as the last step.

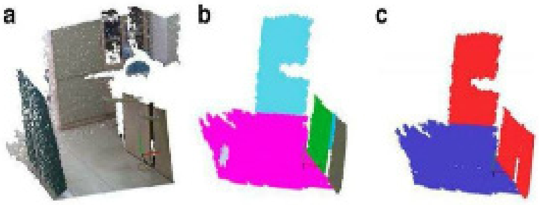


Figure 4. Plane segmentation and ground and wall detection results: a point cloud; b segmented planes; c detected ground (in blue) and wall planes (in red)[15]

The work [16] is also using the Kinect sensor but in addition to creating the depth map it uses typical image feature detecting algorithms like Sobel edge detector to detect edges clearly, and Harris & Stephens detector to detect the corners of the objects in the vision and finally blobs that shows the optical flow is detected using the SIFT detector.

III DISCUSSION

This section of the paper provides a brief discussion on the works, there pros and cons, suggestions and challenges we studied in early chapter. First it is better to summarize about the different approaches for the vision based obstacle avoidance and assistant systems because it is easy to compare and contrast to identify their plus and weak points after summarizing all the systems. In the following table we will categorized the system according to the technological approaches they used and the advantages and disadvantages of those approaches.

When comparing the different technical approaches mentioned above, they have their own advantages and disadvantages. A highly acceptable system should consider about technical factors or functional requirements like reaction time, accuracy, reliability as well as the non-functional requirements like usability, mobility, cost, etc. But achieving this requirements is a challenge due to many reasons.

A *Cost*

Generally, the visually impaired community is lower paid than others so the cost of the device is a critical fact for them. The vision module (camera or sensors), the processing unit (computer or microcontroller) and, the power supply will be the main components that affect the final cost. By using technologies that use lower computing power, we can complete the system with a low-power processing unit. Also, it is important to use technologies that use low-cost vision modules (unlike costly vision modules like stereo cameras).

B *Size and Mobility*

Since these systems are traveling assistant systems, they have to be small in size with higher portability and it is better if the system could be developed as a wearable device. But the challenge is most of the technological approaches need high computing power and need to operate in real-time so most of the times it is necessary to move for larger computers or microcontrollers and that will be a challenge to make the system smaller. The other main factor is since we need to operate these systems in outdoor traveling for a longer time we need to add larger batteries for more battery capacity.

C *Require Higher Accuracy*

The result of an error in this kind of system can be critical. So the system must provide very high accuracy and reliability to the user.

So we need to find the best approach to achieve the given requirements while facing those discussed challenges. When we consider about the physical design of the systems, smart wearables with low weight is always gives more mobility and for any kind of place. But the heavy systems like navigation robots can't be used in places like staircases. And when consider about the sensor and vision modules single camera module are cheaper than stereo camera modules and for distance measuring, sensors with laser technologies always give more accurate outputs and more range but higher on cost. So we need to select the sensors carefully according to our needs so we can develop a high reliable, accurate assistant device with high usability to address the day today travelling problem of visually impaired people.

The following table will facilitate you to compare the relatable have a clear idea about the relatable technologies, used module and the advantages and disadvantages of each technological approach.

IV CONCLUSION

Travelling is one of the main problems facing by the visually impaired community in their day to day lives. Although lot of assistive technologies are available, most of them are not user-friendly for visually impaired people because of the Disability Digital Divide gap. It is hard to use mobile applications and web based applications specially for visually impaired people. So smart wearable devices has to come forward to help them in their day today travelling and develop the navigation capabilities. Vision based obstacle avoidance and assistance technology is the most popular approach to address this problem. The related works shows us it is important to use technologies with high

Table 1. Monocular vision with machine learning other algorithms

Technological Approach	Description	Modules Used	Advantages	Disadvan-tages	Refere-nces
Deep learning models	Deep learning approach can give accurate localization and navigation instructions. Recurrent Neural Network and Convolutional Neural Network is used in training and recognition process.	Camera, Ultrasonic Sensor	Low reaction time(50ms), High Accuracy, Low cost	Complex training process	[5] [6] [7]
Image processing techniques and other algorithms	By using the image processing techniques which identify edges, lines, corners and identifying obstacles using them.	Monocular Camera	Low cost	Low accuracy when comparing with other techniques	[8]
Reinforcement learning	Collect thousands of images with a laser range scan which gives the nearest obstacle in each direction of the image. Using that dataset, train the system with a supervised learning algorithm. It gets more accurate with larger datasets.	Monocular Camera	High Accuracy, Low cost	Need very large data set for higher accuracy	[12]

Table 2. Special Camera Technologies and Sensors

Technological Approach	Description	Modules Used	Advantages	Disadvan-tages	Refere-nces
Stereo imaging	Calculating 3D coordination using two images captured at the location buy from two cameras. And create the disparity map and estimate the ground plane for detect the obstacles.	Stereo Cameras	Not too complex, Low cost	High cost for the vision module (stereo cameras)	[9] [11]
Cabot, Navigation robots	Robots (not wearable) developed with main vision module with many sensor modules for scan and identify the obstacles.	Cameras, Ultrasonic sensors, LiDAR, Laser technologies	High reliability	High Cost, Less mobility	[13] [14]
Vision and Depth sensors	These systems are designed with depth and vision combined sensors like Kinect sensor which make it easy to calculate x, y, z coordinates and optical flow for detect obstacles edges, corners and ground plane.	Kinect sensor, Depth sensors	Low reaction time	Sensitive to infrared and highly reflective objects.	[15] [16] [17]

accuracy and reaction time but also need to have high usability, mobility and low cost. The computer vision systems with deep learning, reinforcement learning, enhanced image processing techniques with relevant cameras or sensors have given acceptable solutions for the addressed problem in the related works. With adding relevant upgrades with the newly updated technologies to those systems, they will give fair service for visually impaired community to make their day today travelling easier and efficient.

REFERENCES

[1] World Health Organization, "World report on vision," p. 180, 2019.

[2] A. Rodrigues, H. Nicolau, K. Montague, J. Guerreiro, and T. Guerreiro, "Open Challenges of Blind People using Smartphones," ArXiv190909078 Cs, Oct. 2019, Accessed: Oct. 24, 2021. [Online]. Available: http://arxiv.org/abs/1909.09078.

[3] H. H. Qureshi and D. H.-T. Wong, "Problems Facing by Visually Impaired People during Interaction with Mobile Applications," p. 8, 2019.

[4] N Wedasinghe, N Sirisoma, APR Wicramarachchi, "Web Mobile and Computer Accessibility: Issues Faced by Sri Lankan Visually Impaired Community," 11TH Int. Res. Conf., Sep. 2018.

[5] D. K. Yadav, S. Mookherji, J. Gomes, and S. Patil, "Intelligent Navigation System for the Visually Impaired - A Deep Learning Approach," in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, Mar. 2020, pp. 652–659. doi: 10.1109/ICCMC48092.2020.ICCMC-000121.

[6] F. Ahmed, M. S. Mahmud, and M. Yeasin, "RNN and CNN for Way-Finding and Obstacle Avoidance for Visually Impaired," in 2019 2nd International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, Jun. 2019, pp. 225–228. doi: 10.1109/ICDIS.2019.00041.

[7] J. O. Gaya, L. T. Goncalves, A. C. Duarte, B. Zanchetta, P. Drews, and S. S. C. Botelho, "Vision-Based Obstacle Avoidance Using Deep Learning," in 2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), Recife, Brazil, Oct. 2016, pp. 7–12. doi: 10.1109/LARS-SBR.2016.9.

[8] D. Croce et al., "An Indoor and Outdoor Navigation System for Visually Impaired People," IEEE Access, vol. 7, pp. 170406–170418, 2019, doi: 10.1109/ACCESS.2019.2955046.

[9] A. Rodríguez, L. M. Bergasa, P. F. Alcantarilla, J. Yebes, and A. Cela, "Obstacle Avoidance System for Assisting Visually Impaired People," p. 7, 2012.

[10] A. Rodríguez, J. J. Yebes, P. Alcantarilla, L. Bergasa, J. Almazán, and A. Cela, "Assisting the Visually Impaired: Obstacle Detection and Warning System by Acoustic Feedback," Sensors, vol. 12, no. 12, pp. 17476–17496, Dec. 2012, doi: 10.3390/s121217476.

[11] P. Costa, H. Fernandes, P. Martins, J. Barroso, and L. J. Hadjileontiadis, "Obstacle Detection using Stereo Imaging to Assist the Navigation of Visually Impaired People," Procedia Comput. Sci., vol. 14, pp. 83–93, 2012, doi: 10.1016/j.procs.2012.10.010.

[12] Jess Michels, Ashutosh Saxena, Andrew Y. Ng, "High Speed Obstacle Avoidance using Monocular Vision and Reinforcement Learning," 22nd Int. Conf. Mach. Learn. Bonn Ger., 2005.

[13] G. Capi and H. Toda, "Development of a New Robotic System for Assisting Visually Impaired People," Int. J. Soc. Robot., vol. 4, no. S1, pp. 33–38, Nov. 2012, doi: 10.1007/s12369-011-0103-1.

[14] J. Guerreiro, D. Sato, S. Asakawa, H. Dong, K. M. Kitani, and C. Asakawa, "CaBot: Designing and Evaluating an Autonomous Navigation Robot for Blind People," in The 21st International ACM SIGACCESS Conference on Computers and Accessibility, Pittsburgh PA USA, Oct. 2019, pp. 68–82. doi: 10.1145/3308561.3353771.

[15] V.-N. Hoang, T.-H. Nguyen, T.-L. Le, T.-H. Tran, T.-P. Vuong, and N. Vuillerme, "Obstacle detection and warning system for visually impaired people based on electrode matrix and mobile Kinect," Vietnam J. Comput. Sci., vol. 4, no. 2, pp. 71–83, May 2017, doi: 10.1007/s40595-016-0075-z.

[16] N. Kanwal, E. Bostanci, K. Currie, and A. F. Clark, "A Navigation System for the Visually Impaired: A Fusion of Vision and Depth Sensor," Appl. Bionics Biomech., vol. 2015, pp. 1–16, 2015, doi: 10.1155/2015/479857.

[17] K. Yelamarthi and K. Laubhan, "Navigation assistive system for the blind using a portable depth sensor," in 2015 IEEE International Conference on Electro/Information Technology (EIT), Dekalb, IL, USA, May 2015, pp. 112–116. doi: 10.1109/EIT.2015.7293328.

[18] D. Holz, S. Holzer, R. B. Rusu, and S. Behnke, "Real-Time Plane Segmentation Using RGB-D Cameras," in RoboCup 2011: Robot Soccer World Cup XV, vol. 7416, T. Röfer, N. M. Mayer, J. Savage, and U. Saranlı, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 306–317. doi: 10.1007/978-3-642-32060-6_26.

ACKNOWLEDGMENT

This review would not have been possible without the great support given by my two supervisors Mrs. G Shanmuganathan, and Dr. B Hettige by educating and correcting me in every step to the final paper. And my grateful thanks goes to Faculty of Computing, General Sir John Kotelawala Defence University for giving me the learning opportunities and facilitating me to collect all the resources.

AUTHOR BIOGRAPHIES

KLH Imesha is a 4th year Computer Engineering undergraduate in Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka. The author is interested in Computer Vision, Deep Learning and Embedded Systems and the related fields.

Gayamini Gnanasuganthan working as a Lecturer (Prob.) in the Department of Computer Engineering, Faculty of Computing, General Sir John Kotelawala Defence University. This author was awarded the M.Sc. degree in Computer Science and Technology from Wuhan University of Technology, Wuhan, P.R. China in the year 2020. Her current research interests lie in Artificial Intelligence, Multi-agent systems, Machine Learning, IoT and Robotics & Automation.

B Hettige is Head of the Depart-ment of Computer Engineering, Fac-ulty of Computing, General Sir John Kotelawala Defence University. His research interests include Multi-Agent Systems, Machine Translation, Sinhala Language and Computational Grammar.

Date of publication July 31, 2022, date of current version Aug. 12, 2022.

Improving Customer Experience in Supermarkets: A New Approach based on Travel Path

RSN Dilrukshi [1#], HA Caldera [2]

[1,2]The University of Colombo, School of Computing, Sri Lanka
[1#] rsnirma@gmail.com

ABSTRACT In today's competitive market, understanding its customers is a key to the success of any business. The market contains various customer subgroups that can be distinguished based on purchasing habits, time spent, product selection, and travel path. To identify the pattern hidden inside these subgroups, is needed to use real data as it reflects the ordinary behaviour of the c ustomers. Analysis of the travel path data that customers make inside the shopping mall enables retailers to understand and predict customer behaviour, which has become a critical point in effective decision making for increasing sales with more customer comfort. Introducing the right discount for the right products acts as an important mediating factor in the customer relationship. Traditional methods of determining the discount and layout have dealt only with customer transactions, which have missed other important characteristics of customers' purchasing behaviour. This paper addresses the problem of sales increase based on personalized discount schemas and improved store layout using customers' shopping travel paths. It uses the Frequent Pattern Growth (FP Growth) algorithm to improve the sales and the RFM (Recency, Frequency, and Monitory value) analysis to identify the customer segments based on the dataset of Instacart from the Kaggle website. An FP growth algorithm has been used to identify the frequent locations and frequent products of a customer's purchases. An improved version of the supermarket layout has been suggested based on the frequent travel paths of customers. The findings of this approach can be used by retailers to improve the in-store shopping experience of customers.

INDEX TERMS: personalized discount, shopping path, travel path, supermarket layout

I INTRODUCTION

Shopping is one of the main investments of energy that people make for their benefits. As technology gets updated with new trends, retailers try to make their customers' shopping experiences more and more interesting and easy. In order to identify and understand the different needs of customers, customer segmentation techniques, which are commonly based on purchase behaviour, time spent on purchase, and purchase history, have been used. The findings have allowed to provide better services and preferable products to customers. These segmentation techniques allow to create profitable segments based on competitive advantages [8]. But identifying the segments based on suitable measures and determining the right marketing campaigns are challenging tasks for markets.

The term "competition" in retail refers to the rivalry among retailers who are keen to retain their customers and attract new ones. The most common and well-known method of improving sales and revenue for retailers with customer satisfaction is by providing discounts to customers. Discounts are typically assigned to items that are not frequently purchased by many customers, regardless of whether they are interested in them. Enabling a discount alone for non-frequent items and keeping them in the original location of the layout do not affect the improvement of the sales of that item. Product placement and layout also play a major role in improving sales in supermarkets because a typical customer decides their next return to the store based on their experience and impression of the current layout of the store. From the perspective of the retailer, the effectiveness of the layout of the store determines the level of the customer's exposure to the goods and affects the chance of the item being bought. The layout design has a direct impact on the travel paths of customers who are searching for their needs inside the supermarket. Therefore, the customer travel paths can be used as a measure to identify the customer's behaviour when buying products, which opens up a new way of increasing sales by analyzing the related data.

This paper proposes a novel approach to improve the sales of the supermarket based on the customer's travel path. A dynamic discount will be calculated for each customer based on their travel path, and a personalized supermarket layout will be suggested by placing the non-frequent sale items in frequent customer travel locations in order to improve the sales. The paper suggests the possibility of improvement in sales and design a personalized supermarket layout by applying the FP growth algorithm to the customer travel path data.

The remainder of the paper is organized as follows: section II provides discussions on shopping analysis of past literature, the proposed methodology is presented in section III , section IV bring out the result and generates a discussion on the findings and lastly, section V concludes the paper with conclusion and future work.

II LITERATURE REVIEW

Innovating marketing strategies are needed in order to create a long lasting and profitable relationship with customers in today's business world. The most salient issue in designing a marketing strategy is that the variation of customer needs from one to another is significantly different. As a result, customer segmentation based on their features and behaviours play a key role in business viability.

A Customer Segmentation

Customer segmentation has led to a deeper understanding of the customer's buying pattern [3]. It costs five times more to acquire a new customer than it does to keep an existing one, and ten times more to re-engage a dissatisfied customer [14]. As many companies focus more on improving their marketing strategies to enhance their market share, they primarily focus on customer segmentation. Dividing the customers into clusters based on their behaviour parameters can lead to a significant growth in their revenue [3]. Segmentation is a key area for retailers as it allows them to identify profitable groups and to organize marketing campaigns accordingly [8].

Considering the data of 250 bank customers, research found five different clusters, which are different based on factors such as loan amount, degree of loyalty, account balance, default risk, and profitability for the bank [3]. Findings suggest that customer clustering can help the financial sector because it augments their competitiveness to improve their marketing methods to target segment-based marketing approaches.

The RFM model has been widely used by researchers for customer segmentation. RFM analyses the behaviour of the customer based on Recency (R) – how recently a customer has made a purchase, Frequency (F) – How frequently a customer buys and Monetary (M) – How much money a customer spends on purchases [5] [7] [10].

A case study defines RFM as a three-dimensional way that is used for classifying or ranking customers, which is based on the 80/20 principle that 20% of customers bring 80% of the revenue of a company [1]. They used RFM to study the scoring of the active e-banking users. In this study, it used clustering as a technique for data mining and organized the findings into cluster groups based on the pyramid model. They used a two- step clustering method to identify the most important customers. The pyramid model has been useful for different businesses because it improves issues such as decision making, future revenue forecast, simulation of inactive customers, and prediction of alteration of the customer position in the pyramid [1].

B Shopping path Analysis

Retailers foremost concern is the shopping layout as it defines the way of customers expose to the products. According to a study, retailers try to expose many products through layout as it enables higher exposer rate, sales and return on investment [12]. Customers want store to create the layout in a way that minimizes this unwanted steps and motion in the shopping process [4]. Common layout design is based on the product category approach where products that share the same functional characteristics or origins are placed nearby. But according to this approach, it failed to respond the needs of the time pressured consumers of the shop. To satisfy the consumer, store sections need to be redesigned based on the consumer desire. Consumer's desire can be identified by analysing their demographic and transactional data. These data only provide the basic information such as quantity and purchase amount and how often they visited and etc. However, to understand consumers' behaviour completely, it needs more data and data mining techniques.

Based on the regional analysis on customer purchase history or recommending products through customer segmentation will not provide sufficient information to understand the customer shopping behaviour in the physical store [11]. To overcome these problems, they used longest common subsequence (LCS) which provide the capability of identifying hotspots where most of the customers visited and dead spots with few visits.

As a result of technological advancements in recent years; RFID, Bluetooth beacons, video cameras and Wi-Fi location tracking have been used for analysis of the customer behaviours inside the super markets. A research was done by Sorensen Associates based on a dataset that collected by tracking the travel paths of customers inside the actual supermarket in western United States [13]. For path tracking they used grocery carts which attached a RFID tag to the bottom. They categorized the path travel by each shopper using clustering algorithm and identifying 14 different canonical paths of it. Through the research they have identified that area at the entrance, end cap of aisles and checkout areas get more attention of the customer. Identification of the pattern in customer behaviour inside the supermarket will result to classify the frequent paths or locations travelled. Pattern discovery from a sequence of data is one of the main tasks in data mining research area. Extract hidden information from large database and then generate association between the items in it defined as association rule mining [2]. Market basket analysis is the common implementation in this method. Through this method it produces association rules which measures the dependency of each item in a dataset [9]. Association rule contain with mainly two parts: an antecedent(if) and a consequent (then). In order to identify the strength of an association rule mainly two measures 'Support' and 'Confidence' are used. Association rules were used to extract the knowledge from a transactional dataset which a shopping layout based on the association among the product categories is suggested [4]. They used Apriori algorithm with dimensionally reduction for identification of the association rules of transactional dataset. They allowed retailers to cluster the products based on the consumers buying habit and to create a strong appeal for the consumers' needs. As an example, rather than placing the coffee in the beverage section, ham in the meat section they suggested to place these products in breakfast food section which allocated for foods related to breakfast. In this paper the authors proposed a method of clustering the different product categories into same section based on the products that customers bought together.

The Frequent Pattern Growth algorithm is another algorithm that is used for frequent pattern mining [6]. By applying the FP growth algorithm in a step-by-step process, it removes unnecessary data and improves the performance of the overall process [2]. The generation of rules in FP Growth must be accompanied by a validation process to ensure that they are applicable and authentic.

By combining the advantages of FP growth with Apriori, an algorithm called Search Space Reduction (SSR) was introduced [15]. In SSR, it first scans the transactions once to count the support and identify frequently occurring items that are higher than the minimum support threshold. Then it generates an FP Tree using the identified frequent item sets. As a result, there is only one item-prefix tree in the memory at a time. In SSR, it uses the function Item-prefix-tree-construction for constructing item-prefix trees and it uses the function Frequent-pattern-generation for candidate generation and frequent pattern generation.

III METHODOLOGY

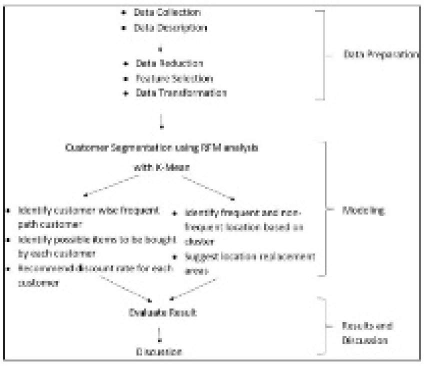

Data Collection
Data Description
Data Reduction
Feature Selection
Data Transformation
Data Preparation
Customer Segmentation using RFM analysis with K-Mean
Identify customer wise frequent path customer
Identify possible items to be bought by each customer
Recommend discount rate for each customer
Identify frequent and non-frequent location based on cluster
Suggest location replacement areas
Modeling
Evaluate Result
Discussion
Results and Discussion

Figure 1. Work flow of the proposed approach

This paper proposed a solution to the above identified problem in the introduction section through RFM analysis and a frequent pattern growth algorithm. The proposed methodology includes three major phases: Data preparation, Modeling and Result and Discussion. Figure 1 shows a general model of how the data is acquired and data analysis is conducted in order to construct the proposed solution.

A Data Preparation

This study incorporates data regarding the customers' transactions and synthetically generated travel path data related to a dataset of Instacart from the Kaggle website. The dataset contained around 1 million grocery orders, which were placed by around 3500 users. It includes details based on the customers' transactions, products with assigned departments, aisles of products, and the shopping path of customers. The initial layout of the shopping mall is synthetically designed, and the layout is divided into sub partials with an assigned location code. Even though the original dataset contained around 3 million records, because of the hardware limitation, for the analysis, around 3000 users with their transitions were selected.

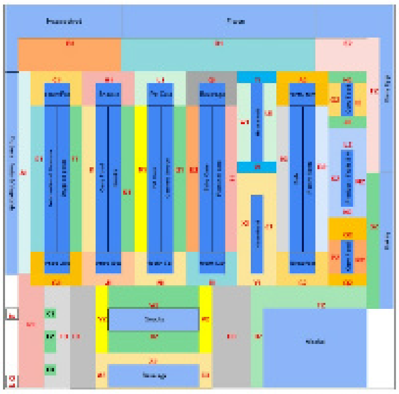


Figure. 2: Layout of the shopping mall

Figure 2 illustrate the layout of the shopping mall with each area assigned with a particular code. This code was used to track the path of the user in traveling inside the mall.

B Modelling

Clustering is the process of grouping objects based on their similarity. RFM analysis is used for customer segmentation. Segmentation is done based on the total orders per customer, average days between orders per customer, and average size of the orders per customer (number of products in an order) aligned with recency (R), frequency (F), and monitory value(M) respectively.

Based on these three measures, the selected dataset is clustered using the K-means clustering algorithm. Identification of the best number of clusters or k value in the k-mean algorithm is important as it leads to minimizing the effect of outliers and the best number of clusters (k) are being evaluated based on distortion score and silhouette score. The dataset was inserted into the k-mean algorithm and model performance was calculated using silhouette score first.

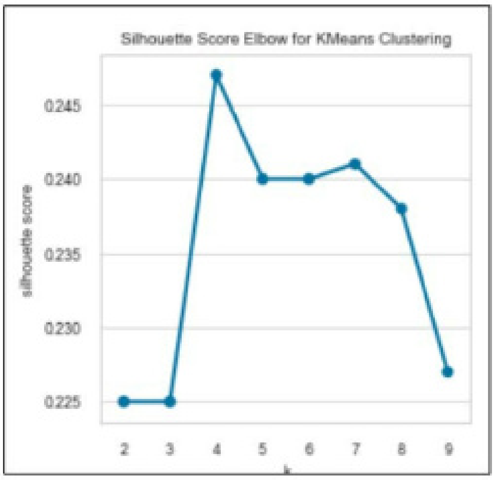


Figure 3: Silhouette score graph

The silhouette score measures how close the point lies to its nearest neighbour points across the clusters by considering the variables such as variance, high-low difference, and skewness. The resultant silhouette score for the number of clusters two to nine was visualized in Figure 3. The Silhouette score reached its' global maximum at k = 4, where it contains an ideal peak value. The best k value for the cluster is four based on the definition of the silhouette score, but for further clarification, the distortion score is also considered.

The distortion score was used in order to clarify the best number of clusters of customers which were identified under the silhouette score. In this method, the K-elbow visualizer is implemented based on the 'elbow' method in k-mean clustering. In this scoring method, the user must first specify in advance the range of clusters, and then the elbow method computes the average score for each cluster. According to the scores plotted in Figure 4, elbow point k = 4 was identified as the best k value.

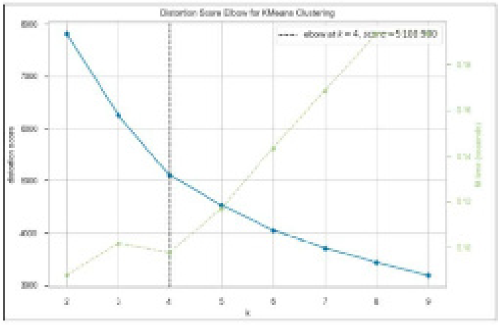


Figure 4: Distortion score graph

K-mean clustering was then concluded with an optimum cluster size of k = 4 for customer segmentation for further analysis.

Figure 5 illustrates the snake plot graph to visualize the average value of the main three features, which are identified in R, F, and M for each cluster. Compared with other graphical data analysis representation techniques, Snake plot graph perform well for customer perception analysis. The labels 'Orders,' "Lag," and "Products" used in Figure 5's X-axis represent the size of the order, the number of days between each order, and the number of products in each order, respectively, and correspond to the recency, frequency, and monitory of RFM analysis.

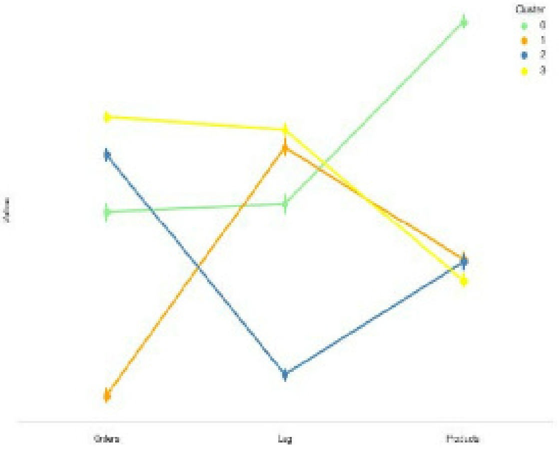


Figure 5: Snake Plot Graph for 4 clusters

Each line represents behavior of each cluster with appropriate scale endpoints for above criteria. Following points discuss each cluster behavior separately.

Cluster 1: Customers who place lowest order rate but not visit the shop often and once visit placed average number of products in an order.

Cluster 2: Customers who place more orders and visit the shop often with each order it contain average number of products.

Cluster 3: Customers who place order most but not frequent with least number of products in the orders when comparing to the other clusters.

1 Frequent path for a particular customer:

By applying the FP growth algorithm to the data of a particular By applying the FP growth algorithm to the data of a particular customer's travelled path inside the mall, his/her frequent path was generated. Figure 6 visualized a heatmap based on the travel frequency for each location by considering the travel path data of customer '516'.

In the heatmap in Figure 6, the variation of the colour areas defined the travel frequency for each location by the customer. Dark-coloured areas defined high travel frequency, while light-coloured areas visualized less travel frequency. By applying the FP growth algorithm to the path data of a customer, frequent itemset are identified for the customer, as illustrated in Figure 7 for customer '516'.

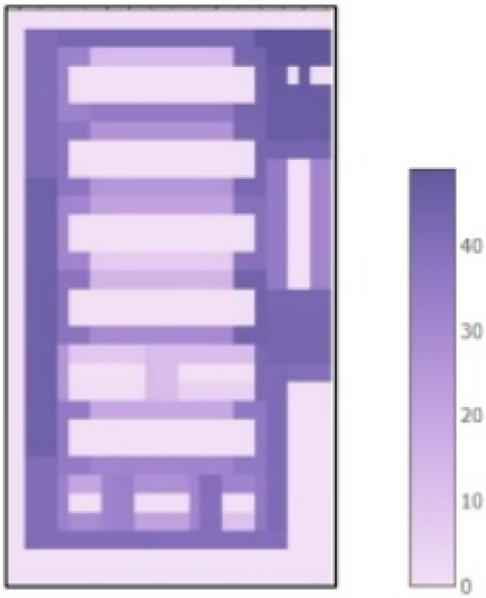
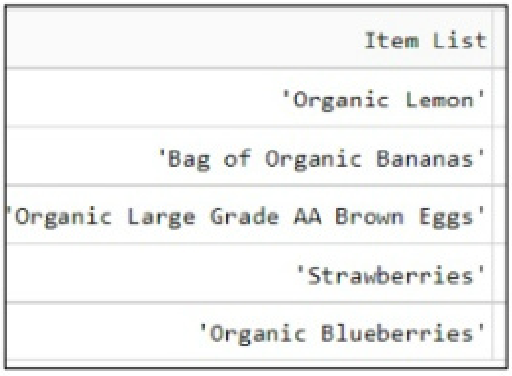
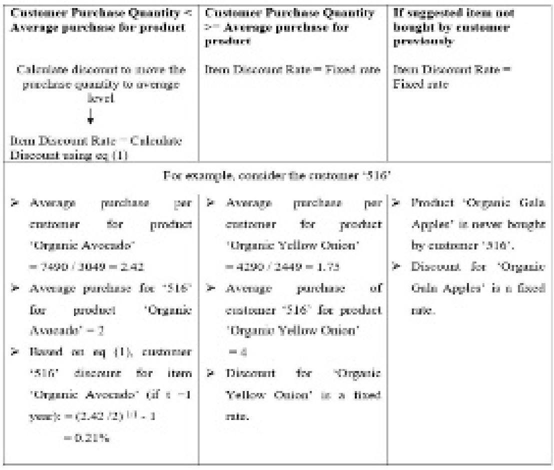


Figure. 6: Heatmap for traveled path of the customer '516'



Item List
'Organic Lemon'
'Bag of Organic Bananas'
'Organic Large Grade AA Brown Eggs'
'Strawberries'
'Organic Blueberries'

Figure 7: Frequent itemset of customer '516'



Customer Purchase Quantity < Average purchase for product	**Customer Purchase Quantity >= Average purchase for product**	**If suggested item not bought by customer previously**
Calculate discount to move the purchase quantity to average level ↓ Item Discount Rate = Calculate Discount using eq (1)	Item Discount Rate = Fixed rate	Item Discount Rate = Fixed rate
For example, consider the customer '516'		
➢ Average purchase per customer for product 'Organic Avocado' = 7490 / 3049 = 2.42 ➢ Average purchase for '516' for product 'Organic Avocado' = 2 ➢ Based on eq (1), customer '516' discount for item 'Organic Avocado' (if t =1 year): = (2.42 /2) $^{1/1}$ - 1 = 0.21%	➢ Average purchase per customer for product 'Organic Yellow Onion' = 4290 / 2449 = 1.75 ➢ Average purchase of customer '516' for product 'Organic Yellow Onion' = 4 ➢ Discount for 'Organic Yellow Onion' is a fixed rate.	➢ Product 'Organic Gala Apples' is never bought by customer '516'. ➢ Discount for 'Organic Gala Apples' is a fixed rate.

Figure 8: Discount recommendation

2 Frequent path for selected group of customers:

Based on the clusters that were identified previously, cluster two was identified as the most effective customer for the revenue of the shop. A sample of 100 customers were selected to apply the FP growth algorithm. By applying the FP growth algorithm to a group of selected customers, their frequent locations were identified.

Frequent Path for 100 customers in cluster 02: K2, E3, V2, A1, N2, D3, C2, E2, G3, Y2, D1, G1, F3, B1, D2, F2, H1, M2

3 Recommendation of the discount:

Discount value for products based on the travel path of user was calculated using following eq(1)[16] and eq(2).

$$\textit{Discount Rate} = \left(\frac{\textit{Expected Rate}}{\textit{Current Rate}}\right)^{1/t} - 1 \quad (1)$$

t – Number of Years

$$\textit{Average Purchase per customer for Product 'ItemName'} = \frac{\textit{Total bought Quantity for the item}}{\textit{Number of items bought by a customer}} \quad (2)$$

Figure 8 illustrate the three scenarios which are considered in discount recommendation.

'Customer purchase quantity' and 'Average purchase for product' is considers as main criteria in discount recommendation.

'Customer purchase quantity': Purchase quantity for particular product by a customer

'Average purchase for product': Average purchase quantity for a product

4 *Layout Recommendation:*

RFM analysis has resulted in four clusters, and among them, RFM analysis has resulted in four clusters, and among them, cluster two was identified as the most important segment for the shop because it includes the high order placement rate, the minimum days between order placement, and each order containing an average size. As this cluster represents the regular visitors of this shop, it was considered for the layout recommendation. In the frequent path, it only includes most of the traveling areas, but not all traveling areas of the customer. If the frequent travel areas include the most travelled areas, customers may tend to buy new products as they travel through the shop. This may result in improved sales and the expansion of the customer's travel areas.

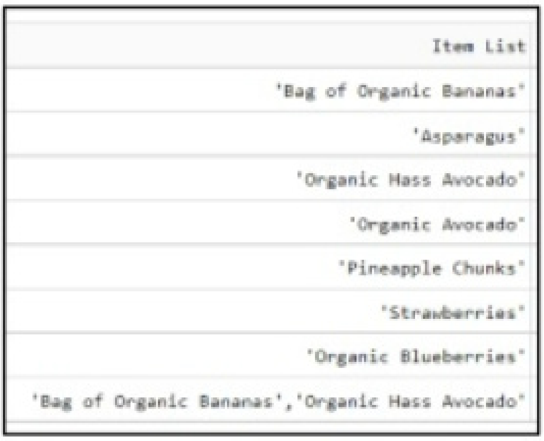
For the layout updating process, a sample of 100 customers from cluster two was selected as it implies the behaviour of all the customers in the cluster and to overcome the technical limitations that will be faced when executing the full dataset at once. By applying FP growth to these customers, the most travelled areas within them were identified. Through this result, the items that are in the most frequent traveling path, infrequent locations, and items that are bought by other customers from frequent locations are identified. Aisles related to infrequent locations can be relocated to the frequent path of the customers. This has allowed to identify the items that are in the relocated aisles and bought by the customers in parallel. By considering the above item lists, it is clear that there are new items in the frequent path that are already bought by customers. When items are in the frequent path of customers, they will tend to buy more products than before. This scenario concludes that relocating aisles will result in increase of sales and enhanced shopping experience for customers.

IV RESULT AND DISCUSSION

A *Improve sales based on discount schema*

Using the FP growth algorithm, it is possible to select the frequent path of a particular customer. This path represents the location codes through which the customer travelled the most in the store during the purchase(s).

In this frequent path, there are locations that are visited by the customer, but items may not be bought from some locations. This research, has introduced a discount schema for items in order to solve this issue. The introduction of discount schemas, may encourage customers to buy products that they have never bought or bought less frequently.



Item List
'Bag of Organic Bananas'
'Asparagus'
'Organic Hass Avocado'
'Organic Avocado'
'Pineapple Chunks'
'Strawberries'
'Organic Blueberries'
'Bag of Organic Bananas','Organic Hass Avocado'

Figure. 9: Frequent Items of customer '626'

When comparing the frequent item list of the customer '626' as depicted in Figure 9 to the customer '516' in Figure 7, the 'Organic Avocado' item is not a frequent item of customer '516'. By introducing a discount for non-frequent items, customers may be more inclined to buy them on their next shopping trip. This led to an increase in product sales and an increase in the revenue of the shop.

B *Effectiveness of current layout over previous layout*

Based on the Figure 2 location codes, Figure 10 illustrates the overall behaviour of the clusters based on the travel frequency of each location inside the supermarket. According to the above Figure 10, each customer group's travel frequency for some of the aisle locations, such as 'W1', 'U1', and 'O2', were lower compared to others.

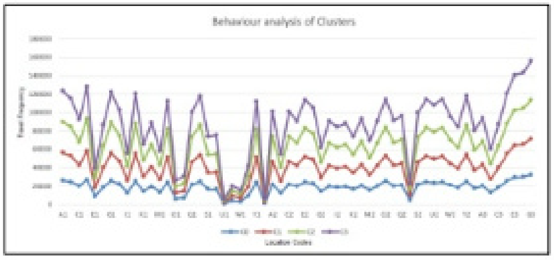


Figure. 10: Behavior analysis of cluster

Locations such as 'A1', 'G1' and 'Y1' contain high travel frequency. Figure 10 concludes that each cluster group has similar behaviour compared to each other for travel frequency inside the shopping mall. Because of that, only a subset of customers from a cluster is considered for layout generation. Based on the previous findings, cluster two was identified as the customer set which is most affected by the layout because of that, hundreds of customers from cluster two were selected for further analysis in the layout for suggesting a process.

Frequent Path for 100 customers in cluster 02: K2, E3, V2, A1, N2, D3, C2, E2, G3, Y2, D1, G1, F3, B1, D2, F2, H1, M2

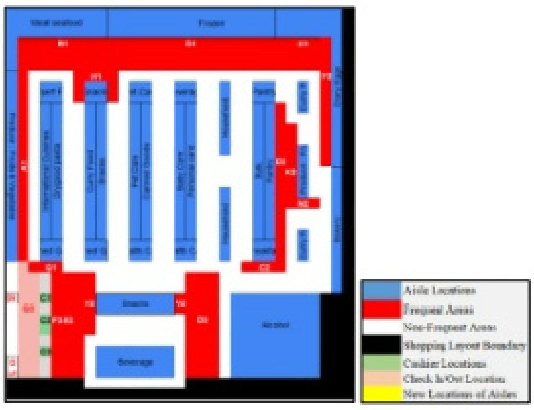


Figure 11: Previous Layout

Figure 11 represents the most travelled areas of the hundred customers who selected previously. Frequent visit areas are represented by the red colour, and white-coloured areas represent less frequent travel areas of customers. According to Figure 11, most of the customers have travelled to the aisles that are placed in the corners of the shop but not to the aisles in the middle of the shop.

According to the location path codes in Figure 2, Figure 12 illustrates the sales of the products by considering 30 path codes. According to Figure 12, a significant number of products which are purchased by customers are located in the frequent path but some of the frequented path locations do not contain a considerable number of purchases. One reason for this could be that even though customers have to travel to some locations, they may not be interested in the items placed there, such as products near the cashier counter, entrance or alcohol area.

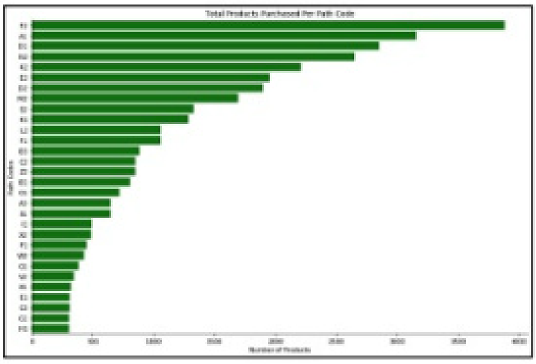


Figure 12: Total products purchased per Path

Relocating the non-frequent sale items to a frequent travel path will result in an increase in sales. Figure 13 illustrates the current layout of the shop, where some of the aisle locations were changed in order to increase sales. Even though some products are bought by the customers, they are not located in their frequent path. However, according to the current layout, they are placed in frequent paths, which may assist customers to easily locating the products and thereby leads to an increase in sales. The layout update mostly affects the customers who visit more often but introducing a discount schema will improve the sales of irregular customers, and their visits.

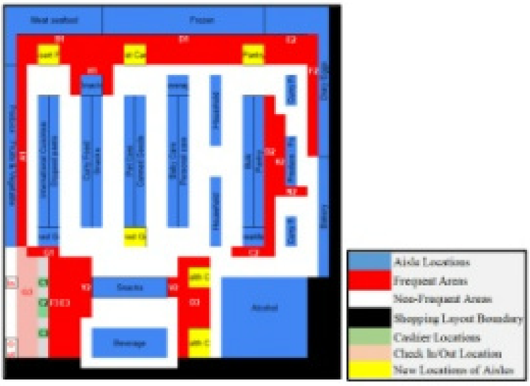


Figure 13: Current Layout

V CONCLUSION AND FUTURE WORK

This project proposed a new discount schema and a new supermarket layout by applying the FP growth algorithm and RFM analysis to travelled path data of customers inside the supermarket. Results are computed based on the supermarket transaction data, which indicates the actual behaviour of the customer. An FP growth algorithm was applied to identify the frequent paths of each customer, from which the frequent and non-frequent areas of customer travel were identified. Consequently, the most frequent items and non-frequent items of the customer were identified. As the suggested discountschemas are based on the customers' travel patterns and are personalized for each customer, they will have a positive impact on the revenue of the retailers. Relocating non-frequent items to the frequent path with discounts will possibly impact the revenue of the shop positively by directing customers to buy more products.

A new shopping layout was introduced by relocating the aisles from non-frequented areas to frequented travel areas, which will allow the customers to easily find their products and also will increase sales simultaneously. Thus, providing a personalized discount based on a customer's travel path improves the sales more than a static discount schema for each and every customer. Our research has finally concluded that recommending discount schemas and shopping layouts based on the travel paths of customers increases sales and improves customer satisfaction at the shop.

Deployment of the research will be a future task. For future research, implementing an advanced pattern mining algorithm in parallel to the FP growth algorithm will improve the performance of result generation. For accurate result generation in path tracking, indoor location tracking techniques can be used. As the suggested discount schemas are for the product categories, they can be further personalized item-wise for a customer and used as an effective discount schema for discount calculation.

REFERENCES

[1] V. Aggelis and D. Christodoulakis, "Customer Clustering using RFM analysis", ICCOMP'05 Proceedings of the 9th WSEAS International Conference on Computers, 2nd ed, 2005, pp. 1-5, [online]: Available:https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.7091&rep=rep1&type=pdf

[2] K. H. Alyoubi, "Association Rule Mining on Customer's Data using Frequent Pattern Algorithm", IJCSNS International Journal of Computer Science and Network Security, vol. 20, issue 5, 2020, 103-110, [online]: Available:http://paper.ijcsns.org/07_book/202005/20200513.pdf

[3] A. Ansari and A. Riasi, "Taxonomy of Marketing Strategies Using Bank Customers' Clustering". International Journal of Business and Management, vol. 11, issue 7, 2016, pp 106-119, doi:10.5539/ijbm.v11n7p106

[4] I. Cil, "Consumption universes-based supermarket layout through association rule mining and multidimension scaling. Expert Systems with Applications", vol. 39, issue 10, 2012, pp 8611-8625, https://doi.org/10.1016/j.eswa.2012.01.192

[5] Y. L. Chen, M. Kuo, S. Wu and K. Tang, "Discovering recency, frequency, and monetary (RFM) sequential patterns", Electronic Commerce Research and Applications, vol. 8, issue 5, 2009, pp 241-251, https://doi.org/10.1016/j.elerap.2009.03.002

[6] C. H. Chee, J. Jaafar, I. A. Aziz, M.H. Hasan and W. Yeoh, "Algorithms for frequent itemset mining: a literature". Artif Intell Rev, vol. 8, issue 5, 2018, pp 2603-2621, doi:10.1007/s10462-018-9629-z

[7] K. Coussement,F. Van den Bossche and K. De Bock, "Data accuracy's impact on segmentation performance: Benchmarking RFM analysis, logistic regression, and decision trees", Journal of Business Research, vol. 67, issue 1, 2014, pp 2751-2758, doi: 10.1016/j.jbusres.2012.09.024

[8] O. Dogan, E. Aycin and Z. A. Bulut, "Customer Segmentation by using RFM Model and clustering methods: A Case study in Retail Industry", International Journal of Contemporary Economics and Administrative Science, vol. 8, issue 1, 2018, pp 1-19, [online]: Available: http://www.ijceas.com/index.php/ijceas/article/view/174

[9] S. Gurudath, "Market Basket Analysis & Recommendation System Using Association Rules", Thesis, Master of Science in Big data Management and Data Analytics, Griffith College, Dublin, 2020, [online]: Available:

[10] Y. Hu and T. W. Yeh, "Discovering valuable frequent patterns based on RFM analysis without customer identification information. Knowledge-Based Systems", vol. 61, 2014, pp. 76-88, doi:10.1016/j.knosys.2014.02.009

[11] I. Jung and Y. S. Kwon, "Grocery Customer Behavior Analysis using RFID based shopping paths data", World Academy of Science, Engineering and Technology, vol. 5, issue 11, 2011, pp. 1508-1512, doi.org/10.5281/zenodo.1081169

[12] O. A. Kasapoglu, "Data Analysis for Retail Layout Decision", International Journal of Advanced Research and Review, vol. 1, issue 6, 2016, pp. 115-126.

[13] J. S. Larson, E. Bradlow and P. S. Fader, "An exploratory look at supermarket shopping paths", International Journal of Research in Marketing, vol. 22, issue 4, 2005, pp. 395-414, https://doi.org/10.1016/j.ijresmar.2005.09.005

[14] R. Soudagar, "Customer Segmentation and Strategy Definition in Segments: An Case study: An Internet Service Provider in Iran", Master Thesis, Master of Arts, Business Administration, Lulea University of Technology, Sweden, 2012, doi:10.1109/ICEBE.2018.00027

[15] S. W. Yen, C. H. Wang and L. Y. Ouyang, "A Search Space Reduced Algorithm for Mining Frequent Patterns", Journal of Information Science and Engineering, vol. 28, issue 1, 2012, pp. 177-191, doi:10.6688/JISE.2012.28.1.12

[16] M. Thakur, "Discount Rate Formula ",EDUCBA, Accessed: Aug 20,2021[online], Available https://www.educba.com/discount-rate-formula/

ACKNOWLEDGMENT

Researchers would like to acknowledge all the staff members of the University of Colombo School of Computing for the guidance and support they have given throughout the research work.

AUTHOR BIOGRAPHIES

RSN Dilrukshi received BSc (Hons) in IT degree from General Sir John Kotelawala Defence University and currently pursuing her master's degree at University of Colombo School of Computing.

HA Caldera received hid PhD degree in computer science from University of Western Sydney, Australia in 2005. Since then, he has been a Senior Lecturer at the University of Colombo School of Computing. His current interests include Data Mining, Web Mining, Business Intelligence and Natural Language Processing. He has published and reviewed many international conference and journal papers.

Date of publication July 31, 2022, date of current version Aug. 12, 2022.

An Android Application to Manage House Rental and Maintenance in Sri Lanka

MTA Wickramasinghe [1#], SHIDN de Silva[2], and D Gunasekera [3]

[1]Department of Information Technology, Faculty of Computing, General Sir John Kotelawala Defence University, Sri Lanka

[1#]36-it-0020@kdu.ac.lk

ABSTRACT The impact of COVID-19 outbreak was felt across all real estate management. A slowdown in the house rental and maintenance management system can be anticipated, as a result of the lock-down and limitations in financing. There is a severe impact on handling the relationship between the house owners, tenants, and the handymen. Property management is a crucial component of being a landlord, but it is far from straightforward. An appropriate methodology was carried out by the researchers to identify all the problems regarding real state property management through quantitative and qualitative data gathering procedures such as semi-structured interviews, face-to-face interviews, questionnaires, and direct observation of the selected sample. After analyzing, the house owner must screen tenants, collect rental fees, handle complaints, and keep tenants satisfied, among other things. In this pandemic situation, tenants faced more difficulties such as difficulty in finding a better house, paying monthly payments, paying utility bills, loss of connection with house owners, and finding the nearest handymen. Handymen suffered a lot mainly because of the inability to find works. Researchers' main aim is to give an appropriate solution for Sri Lankans. By examining the responses this investigation shows that a mobile application would be a better solution than implementing a web application. Iterative waterfall methodology was used for implementing this application. The researchers decided to develop this application using android studio and to enhance the effectiveness of the system by using 360 VR photography, Machine learning (ML)-based technologies, OTP/Fingerprint for User Verification and Geo location, and Geo-tagging.

INDEX TERMS: House Rental Maintenance Management, 360 VR Photography, Machine Learning

I INTRODUCTION

Serious implications have happened with the Sri Lankan economy with the global crisis. The real state sector is the main sector affected due to this pandemic situation. Owing to the changes in the rental market, landlords complained of low rental income and increased risk of losing renters. There are some issues for renters in finding the most suitable house. Compared to other handymen are the people who suffer more from not having a job during these days, even they cannot afford to find money to complete their daily work.//

Therefore, the main aim of the research was to identify the challenges faced by the tenants, handymen, and house owners in the current real estate management systems and give them a solution by implementing an android application for house rental and maintenance management in Sri Lanka.//

Their main objectives of the research were,

1. Analysing the challenges faced by users in current house rental and maintenance management.
2. Examine the current and existing developments which have been done regarding house rental and maintenance management in both Sri Lankan and worldwide contexts.
3. Analyzing the opinion on implementing mobile applications and designing an architecture for implementing a mobile application.

It is especially important to keep an efficient communication between the landlord, tenant, and the handyman, hence the use of mobile phone applications for contact tracing during the COVID-19 pandemic is vital. Accordingly, the researchers have identified that implementing a mobile application is more efficient than developing a web application.

To appropriately determine the processes and house rental and maintenance system user's requirements, quantitative and qualitative methodologies are applied. House owners, tenants, and handymen are the primary sources of collecting data. Data are collected by conducting semi-structured interviews, face- to-face interviews, questionnaires, and direct observations of the selected sample. Secondary data were collected through a survey conducted by house owners and tenants. Factors found to be influencing the real estate of Sri Lanka have been explored using websites and literature of current and past decades. Technologies that were used were 360-degree VR photography in which users interact with and manipulate a simulated real or imaginary environment. Geo-Location & Geo Tagging which are helpful to find a nearby handyman using a variety of location-specific information and to identify the geographic location of the handyman, especifically near the specific house that needs repairing and maintenance service at trying times such as the recent pandemic. OTP/Fingerprint for User Verification, is advantageous when it comes to paying rental payments, utility bills, handyman payments requests because fingerprint identification is unique, highly accurate, and simple to use. Accordingly, identifying all the problems and difficulties faced by Sri Lankans, the researchers proposed an appropriate housing rental and maintenance management application.

II LITERATURE REVIEW

The secondary objective of this research is to examine examining the existing developments which have been done regarding house rental and maintenance management in both Sri Lankan and worldwide context. Researchers used research papers and websites to review the existing developments which have been done regarding house rental and maintenance management in both Sri Lankan and worldwide contexts. Here in this literature review, researchers have analyzed the existing developments which have been done regarding house rental and maintenance management in both Sri Lankan and worldwide contexts.

With the advancement of technology in Sri Lanka, most of the fields involved in the use of automated systems to enhance the performance and the efficiency of the tasks of organizations. However, the usage of automated systems for the real estate sector is low when compared with other developed countries. Nonetheless, it is possible to argue that recognizing possibilities from challenges and transforming obstacles into opportunities is the most strategic course of action in the country's real estate sector at this critical juncture.

And with the COVID-19 pandemic [19] the need for automated systems has arisen than the previous era. A considerable amount of literature has been published on property management systems all around the world and in Sri Lanka in past few years. This study [1] examined the current use of computer softwares in the New Zealand residential property management industry, as well as property managers' perspectives and experiences with the program. Property management software solutions handled a wide range of tasks, including tenant database management, rent roll and payment processing, vacancy management, maintenance of record keeping, financial accounting and reporting, and tenant communication. To find out what factors were most significant to survey respondents when choosing their company's property management software, they were given a list of major software characteristics and asked to rate how important each one was when choosing their current program. Reporting capabilities, ease of use, technical support, security processes, flexibility, communication capabilities, scalability, data storage and retrieval, maintenance activities, and software cost were all high-ranking qualities. However, it was recognized as one of the areas in which property managers were the least satisfied and had issues. The issue was discovered to be not with the technical support service itself, but with the difficulties of contacting the technical support service. In the past two decades, number of researchers [2] have sought to determine rent house management systems with basic technologies. Existing systems have basic features such as using the command buttons to manipulate the database, having the ability to add deleting viewing, and inserting data. The role of object-oriented programming and the role of relational database management system managing mostly important task. The systems have very simple interfaces only with the details of the tenant and the property owner.

The evidence of the research [3] resulted in the creation of a web-based housing management system. The system's purpose is to manage senior staff housing and to make it easier to apply for and update housing. It also enables the housing unit to gain simple access to data, boost productivity, and reduce manufacturing costs. The approaches utilized in this study were Adobe Creative Suite 5, which was used to construct the front end, while CorelDraw Version 15 was used to design the visuals on the pages, and XAMMP Server version 5.3.5, which had PHP and MySQL applications, that were used to make the site pages dynamic. Housing management systems are intended to handle data, keep track of it, and enable quick access to accommodation applications. This is necessary to establish decision-making procedures and institutional arrangements. However, suggestions for further enhancement were given, such as including a mobile alert and payment system notification. Problems of the existing system were typically characterized by paper-based information management practices. The advantages which have been identified by maintaining a web-based application were easy deployment, security, highly economical, cross-platform compatibility, and easy access to the database.

These studies discussed the study of the implementation of android applications for housing society management. Throughout the android platform, this project mainly used "Push notification Technology". This study [4] shows that the disadvantages of the existing system such as unreachable information, lack of authenticity and reliability and high time consumption. This paper proposes a smarter way of communication, fruitful solutions for day-to-day problems. This application-based on the mobile platform it uses MVC architecture.

The most obvious finding that emerged from this study is [5] researchers establish a web application that helps the user to register an individual home or apartment to assist you to find the perfect rental home or property for search view in your target area. Understanding how exhausting it is to contact individual property agents, schedule appointments, and supply better service this application was designed. This website is designed to fulfill all the needs from buying property, selling property, leasing the property.

This study of the application [6] focuses on building a better relationship between buyers and sellers by simplifying many tasks such as mainly focusing on the nearest location prediction, identifying the vacant places, sending automatic rent reminders, package notifications, utility bills, emergency info, location information. In the extended system added the GPS in build and gave a live chat online option. Java script technology was used for implementation. The suggested approach supposes security mechanisms using a distance-vector algorithm including the message exchange and updates message security authentication mechanism without introducing significant network overheads and complexity.

A considerable amount of literature has been published on mobile applications for real estate management in various countries. These studies [7] presented a model mobile application to the automated monitoring system to determine the quality of housing to check the performance of low and medium costing and its assessment. The study briefed about the transformation of empirical housing data into the integrated software to determine housing quality. This study identifies the design quality indicators and parameters for affordable housing in Karachi Pakistan. The context of quality indicators for housing design are classified under various segments of housing design components. Using mobile applications in housing sector has been advantage for proposing a conceptual model for the building designing, proposing a model for selection of interior furnishing and floor covering materials and developing an automated building element selection system.

This research [8] extends knowledge on recent developments for locating the available handyman services within a locality identifies the advantage of having a mobile application that helps in streamlining the process of acquiring a handyman. This study applied agile methodology as software technology. handyman location details were obtained by GPS. The study [9] has confirmed a recommendation system that allows the users to hold out a preference-based cooperative filtering search on rental properties which preferences based on shallow learning, which could be applied to ease the task of locating the desired things online. AR and Vuforia are also used to visualize the space. The system was designed as an internet application victimization handlebar for the front-end and Nodes-ExpressJs for Back-end. The system performs better than existing algorithms and predicts better in a memory-based approach.

Recent evidence [12] suggests the solutions for proving adequate public rental housing (PRH) with decent quality and desirable location. This study utilized a machine learning technique called long short-term memory (LTSM) to construct a set of housing price prediction models which indicate the proximity to impact on nearby housing prices at the city. The approach taken by the study can facilitate improving the PRH policies and programs.

The first serious discussions and analyses of the study [13], technologies that were used to improve the efficiency of real estate management applications emerged during 2019. Disruptive digital technologies are a necessary part of today's reality. These technologies are converting traditional industries into more innovative and adaptable ones around the world. The situation of global real estate, on the other hand, has failed to improve and it is currently falling behind the technological curve. As a result of this latency, the relevant information is either not made available to end-users or is shared too late, resulting in an increased risk. Users of internet real estate platforms have expressed their concerns. As a result, there are more vacancies and post-occupancy regrets among the service providers.

The Big9 technologies, which include drones, the internet of things (IoT), clouds, software as a service (SaaS), big data, 3D scanning, wearable technologies, virtual and augmented realities (VR & AR), and artificial intelligence and robotics, are assessed and identified as the new technologies that are used for real estate management.

The RESTAM framework, which focuses on online platform-based real estate users, is expected to lay the groundwork for introducing the missing technology acceptance model for real estate stakeholders, so the real estate business is transforming traditional to smart real estate because of Big9 disruptive technologies. This will lessen real estate service users' post-occupancy regrets and improve relationships amongst diverse real estate stakeholders.

The empirical study [11] found new methods for creating information-rich interactive 3D environments that are increasing in demand as virtual reality (VR) and the corresponding 3D documentation and modeling technologies evolve into increasingly powerful and proven tools for numerous applications in architecture, monument preservation, conservation/restoration, and the presentation of cultural heritage. The researcher discusses the creation of an immersive virtual reality application for the Imperial Cathedral in Königslutter, in which 360° panoramic pictures were merged as a novel and complementary method of visualization within the virtual world. So those empirical studies which were published open a path for a researcher to establish this implementation.

Referred [20] shows that the details on the real state app development companies in Sri Lanka. The architecture and the design that there used are much valuable for this research.

III METHODOLOGY

For an explicit research methodology, adapting the research onion model for this study is much efficient for the researchers. Research philosophy of this research is based on finding the best-suited android application for house rental maintenance management of Sri Lanka. As an ongoing research, it adheres to the view that only factual knowledge is gained through the observations and measurements, the researcher conducts a positivism research philosophy. A deductive approach was conducted by the researchers through this research, by through examining the existing application on real estate management of Sri Lanka which was invented and used by the expertise.

As the researcher mentioned previously, the first objective of this research is to identify and analyze the challenges faced by users in current house rental and maintenance management. And the third objective of the research was to analyze the opinion on implementing mobile applications and designing an architecture for implementing the mobile application.

To realise both above mentioned objectives researcher identified a specific set of people for the data collection. The specified audience were Sri Lankan tenants, handymen, and house owners. Researchers decided that the best way of collecting data from a specified audience was through a mobile survey. Then the researcher conducted a mobile survey among a specific group of people. Moreover, the researcher used to have some observations made on the current situation and took some ideas from users by meeting them directly through video conferencing. The firsthand attitudes of the community were collected by using primary sources mainly from semi-structured interviews, face-to-face interviews, questionnaires, and direct observation of the selected sample. Personal records, client histories, and service records gave additional information on existing systems.

The second objective of the research was to examine the current and existing developments which have been done regarding house rental and maintenance management in both Sri Lankan and worldwide contexts. Then researchers review research papers and websites. The analysis of those papers was mentioned in the above literature review.

The researchers used several kinds of research strategies such as conducting surveys on the identified audience, understanding the grounded theories and algorithms which were used, clearly understanding the current scenario, and focusing on the best solution for recovering the problems in the current situation. Researchers use an interactive inquiry technique that combines collaborative problem-solving with data-driven collaborative analysis or research to uncover underlying causes and make predictions about personal and organizational transformation in the future. Background investigation, habits, lifestyle, behavior, mutual differences, and the different perceptiveness of the clients are some parameters used in the investigation of the ethnography. Time horizon takes a major part in research for a while, here a cross-sectional time frame was used to conduct this research at one point in time using different samples of a selected group of people and the snapshots of a given point in time change at a societal level. Requirements for the mobile-based feedback system are collected during the literature review by observing similar types of systems and fact-finding techniques. This system is technically feasible as most of the house owners, tenants, and handymen have a smartphone.

The system is developed using android studio, Android SDK, and NetBeans. The server-side language is Java and database is based on cloud technology. The Google Play store sells Android apps, and researchers are use the Google Pay API to integrate them. The developer even set it up to accept credit cards. The researcher will define the google pay API version to request a payment token for the payment provider. Then developer should define the supported payment card networks and describe all allowed payment methods. Moreover, should create the PaymentClient instance by determining the readiness to pay with the Google Pay API. Then the developer should create a PaymentDataRequest object for registering event handler for user gesture to handle the response object. Iterative waterfall methodology is used during the development of the system as it reduces the developers' effort and time required to detect and correct the errors.

A Sample Population

The population of this research to gather data through questionnaire was selected normally from the people older than 20 years. People have been classified into three categories as house owners, tenants, and handymen. Thus, a nonrandom sampling method was used to select the covering several provinces in Sri Lanka. Among the identified population, about 134 sample participants was selected to elaborate and collect the data while some data was collected through the research papers. In order to maintain high data accuracy, a formal way has been used in collecting data.

B Data Gathering

The survey data for this study was gathered through a questionnaire and literature reviews. The survey was conducted by delivering a questionnaire to publications and websites. This was done to collect 70 customers or tenants, 26 house owners, and 38 handymen and the literature review was completed by consulting 15 research data extremely precisely to improve the effectiveness of the research outcomes.

IV RESULTS AND DISCUSSION

Although the first objective of the research is to identify the challenges faced by the tenants, house owners, and handymen who are involving house rental and maintenance. As a result, the data was gathered by the quantitative approach using a survey. Those results were analyzed by the researcher as mentioned below.

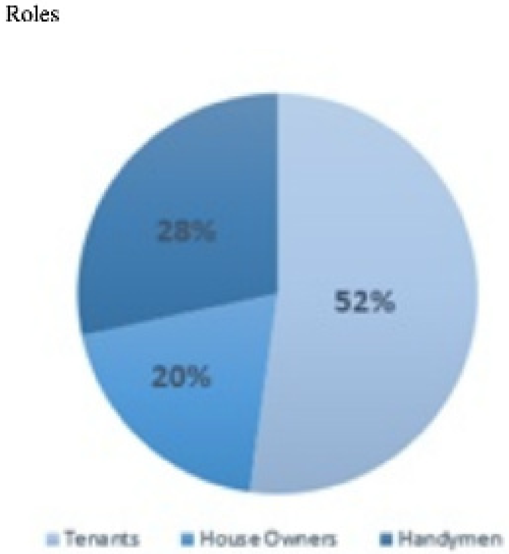


Figure 1. Designation Population Distribution

Analysis and Interpretation: As shown in Figure 1 of the 130 specimens that responded to the survey plurality of 52% were Tenants, 20% were house owners and 28% were handymen.

- Confirmation Statements

Table 1. Confirmation Statement 1

Confirmation 1	Yes	No	Maybe	Total
Facing a lot of challenges for daily life and economy due to covid -19 pandemic	119	2	13	134

Analysis and Interpretation: Table 1 shows the responses of the sample population for confirmation statement 1 and most of the respondents have agreed with the statement by giving all together 132 responses for yes and maybe.

Table 2. Confirmation Statement 2

Confirmation 2	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Total
Opinion on implementing mobile application to overcome the problems in house rental and management system.	91	27	9	4	1	134

Analysis and Interpretation: Table 2 shows the responses of the sample population for the confirmation statement 2. Most of the respondents have agreed with the statement by giving all together 118 responses for agreeing and strongly agree with implementing a mobile application to overcome the problems in the house rental management system.

- Challenges for house owners for their economy due to the covid-19 pandemic.

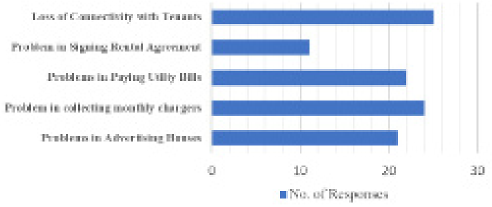


Figure 2. Challenges faced by House Owners

Analysis and Interpretation: Figure 2 shows the Challenges for house owners for their economy due to the covid-19 pandemic. Other than these challenges owners mentioned that it was very difficult to identify the nearest handymen for services.

- Challenges faced by tenants due to the covid-19 pandemic

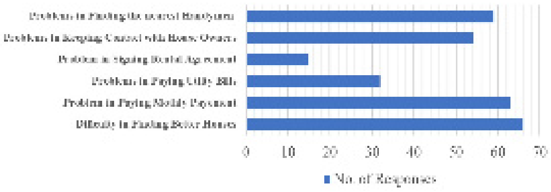


Figure 3. Challenges faced by Tenants

Analysis and Interpretation: Figure 3 shows the samples listed the attitudes on problems faced by tenants.

V REQUIREMENT ANALYSIS

There are four main user types in this system. This proposed system may be accessed by the administrator, house owner, handyman, and tenant using those four unique logins. Furthermore, each house owner and handyman have a unique username and password provided by the system when they register. The tenant can log in with their username and password, which they created when they first registered to the system. There are major functional requirements are listed below. Admin should be able to,

- Perform CRUD operations in the system.
- View house owners, houses, tenants, and handyman's details.
- Remove property advertisements.
- Update and remove owner-related house details and handyman details.

House owner should be able to,

- Add advertisements including house details.
- View appointments of tenants
- Search rented houses and tenants' details.
- View tenants' requests for maintenance.
- Sign house rental agreement with the tenant.
- Do handymen payments if need.
- Change own profile details and password

Tenants should be able to,

- View the properties available.
- Choose suitable houses and create an appointment to meet the owner.
- Choose the nearby handyman who suits their task.
- View the details & contact the handyman.
- Pay handyman payment.
- Sign house rental agreement with the owner.
- Pay house rental fees and utility bills through the app.
- Change their profile details and password.

The handyman should be able to,

- Notifications about the requests.
- Change their profile details and password.
- Add/Update their qualifications.
- Take work from the tenants and house owners.

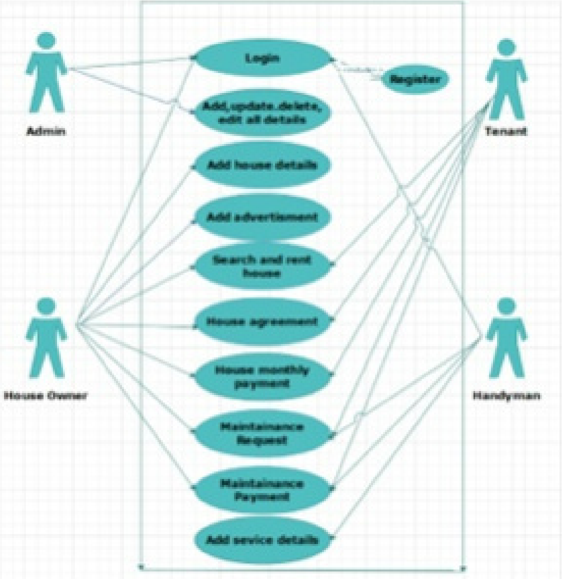


Figure 4. UML Use Case Diagram for Proposed System

VI SYSTEM DESIGN

A Technologies

This mobile application supports the following technologies. The interactive viewing of panoramic images, usually comprising a 360-degree circle or a spherical perspective, is known as VR photography (virtual-reality photography). The art of recording or generating a full scene as a single image, as seen when rotating around a single central spot, is known as virtual reality photography. The entire virtual reality image might be a computer-generated effect, or a mixture of photography and computer-generated objects, and is usually formed by stitching together a series of photographs taken in a multi-row 360-degree rotation or utilizing an omnidirectional camera. To give the best experience for tenants can optimize 360 player experiences for mobile applications, The application supports all panoramic images. Images can be captured with a 360 camera such as Ricoh Theta, Gopro MAX, Insta 360, or DSLR. Images can be rendered using 3D software. House owners could upload and share on the application. The efficiency of the application is increased as VR photography keeps human interaction intact which users interact with and manipulate a simulated real or imaginary environment.

The sole purpose of the smartphone app is to make our lives easier. As a result, when developing an Android application to provide the best handyman service, it's critical to consider the consumers' ease in locating the handymen who are the closest to them. As a result, the most significant feature in this application is the 'Find Nearby Handyman' option. Along with the location selection, it assists users in the following ways.

Machine learning (ML)-based technologies are rapidly being employed in real estate property management to improve service quality and efficiency. In-house rental and maintenance management presents a novel strategy for precisely predicting where the handymen are located. The researcher uses global positioning system (GPS) information from tenants' and house owners' mobile devices as well as Wi-Fi data that covers the whole area. Researchers learn some of the user's behavioural preferences based on the prediction findings. Researchers use these projected handyman locations to give more accurate services to our tenants and house owners.

All these novel technologies that the researchers are supposed to use will enhance the system's performance. Panoramic images which were added using 360 VR photography, will help users to take an accurate imagination of the houses. Further, machine learning, GPS, Geo location and Geo tagging technology, increase the easiness of finding nearby handymen. The authentication level of the application increased by OTP/Fingerprint.

VII DESIGN APPROACH

The house rental and maintenance management system mainly consist of seven main modules. Interactive mobile prototypes were created for each module for efficient the tasks of implementation.

A Registration and Login Module

House owners, handymen, and tenants should register for this system by themselves by entering their username and password as they preferred. Those usernames and passwords are used to log in to the system. If required users can change their passwords after login into their account. Login function should be used to access system users to log into the system. Users should already be with their usernames and passwords.

B Administration Module

The administrator has the authority to access all the house ownersâ€™ details, property details, handyman details, and tenant details. Admin can access the system by adding, editing, and deleting, and removing the users.

C House Rental Procedure Module

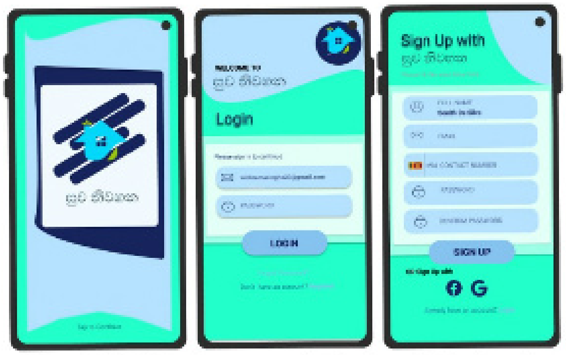


Figure 5. Mobile Prototypes for Login and Registration Module

The system provides the main function as rent a house. Property owners can advertise an advertisement to rent their houses. The owner should enter the house details which are mainly useful for tenants. owner details should be supplied for the contact purpose. House ID is auto generated when posting a house. Tenants can go through those advertisements to choose the best house by contacting using house owner details. Mainly the house owners can capture images of houses using a 360 camera and 3D software can be used for rendering the images. Those photographs can be posted with house details to give a live experience of the house.

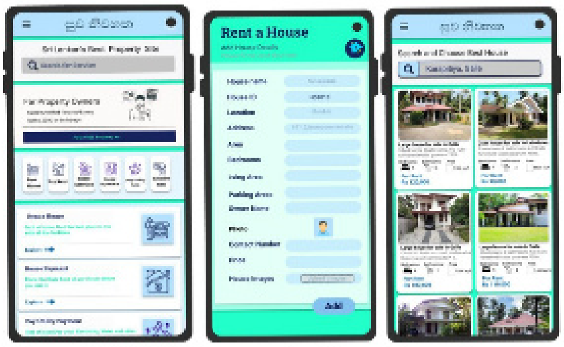


Figure 6. Mobile Prototypes for Rental House Procedure Module

D Handymen Service Module

The main function given by the application is handyman can add their service details to the system on their own. Tenants can go through the relevant service category, and they can find the handyman who can fulfill their request and contact them through using the given handyman details. The availability of the option of nearest handyman, prediction is very helpful during the current situation. The handyman who is available for the chosen service category will be shown on the map with their location.

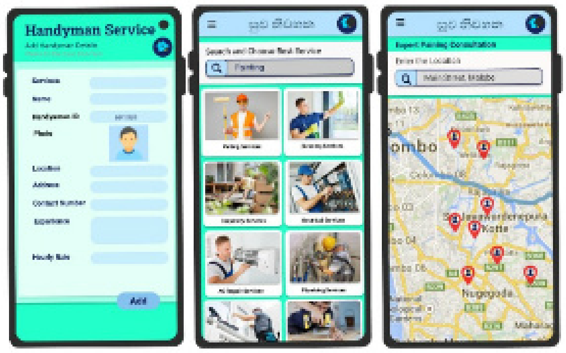


Figure 7. Mobile Prototypes for Handymen Service Module

E Rental Agreement Module

Renting a house according to the rules, regulations, and policies is vital to avoid conflicts. After tenants choose the best suitable house for them, an agreement should be signed between the house owner and the tenant. By using this application that purpose can be fulfilled. The owner and tenant can upload and download those relevant documents and those will be fully secured.

F Payment Module

There should be a connection between the tenant and the house owner mainly for the payment purpose. This application allows the tenants to pay the monthly house rentals for owners with other utility bill payments through the application itself and also handymen service payment can also pay through the app directly. Owner and tenants can pay an advance payment or full payment when requesting a service from the handyman. Tenants can transfer money to the handymen's bank account and the house owner's bank account through this application.

G Notification Module

Reminders, notifications, emails, and messages are compulsory in connecting the users to the application. The system should generate notifications on requests for maintenance service, tenants should be notified with newly posted advertisements, rental house payments, utility bills, and handymen payments. House owners should be notified of rental payment, tenants, and handyman's requests. The handyman should get reminders on their scheduled works, tenants' requests to be accepted or ignored.

After designing the flow of the application, researchers will implement this application. The application should be tested on a sample population and encouraging those users to provide their feedback and suggestions for this application.

Finally, researchers conclude that establishing this application by targeting the real estate users of Sri Lanka will effectively increase the direct communication and engagement between real estate owners and clients, improve customer engagement, create loyalty among users, create competitive advantage, offer an opportunity to provide offer unique services, and create efficient marketing in real estate industry in Sri Lanka.

VIII CONCLUSION & FURTHER WORK

This paper presents a solution to the problems faced by Sri Lankan house owners, tenants, and handymen during this COVID-19 pandemic situation. As the mobile phone is an essential device for people in these days, mobile application takes a prominent place in every industry. For further work researchers would recommend improving this android application with many more options for its users and to address the above-mentioned limitations and it would be more helpful to face the challenges in real estate industry in Sri Lanka during this COVID-19 pandemic situation. For future works, researchers plan to develop the paramedic application activating a mobile application into the IOS platform. Further, this system can be improved by using this application in both Sinhala and Tamil languages and USSD activation mode can be developed in this system as an additional functionality.

REFERENCES

[1] Halvitigala, D., & Gordon, J. (2014). the Use of Property Management Software in Residential Property Management. 20 Th Annual PRRES Conference, 19–22.

[2] Peter Gommans, H., Mwenda Njiru, G., Nguka Owange, A., & Proffessional. (2014). Rental House Management System. International Journal of Scientific and Research Publications, 4(11), 2250–3153. www.ijsrp.org.

[3] Omosebi, P. A., & Adeoye. (2016). Web-Based Housing Management System. First International Conference on Advanced Trends in ICT and Management (ICAITM), April 2016.

[4] Gavhane, S., Vatharkar, R., Sonar, S., & Patil, P. (2015). Study of Implementation of Society Management System. International Journal of Computer Applications, 132(1), 34–36. https://doi.org/10.5120/ijca2015907265

[5] Shriram, R.., & Nandhakumar, P. (2019). House (Individual House / Apartment) Rental Management System. International Journal of Computer Science and Mobile Computing, 8(9), 141–146.

[6] Nandhini, R., Mounika, K., Subhashini, S. M., & Suganthi, S. (2018). Rental Home System for Nearest Place Prediction. 119(10), 1677–1686. http://www.ijpam.eu

[7] Chohan, A. H., Affandi, H. M., Awad, J., & Che-Ani, A. I. (2017). A Methodology to develop a mobile application model to appraise housing design quality. International Journal of Interactive Mobile Technologies, 11(6), 4–17. https://doi.org/10.3991/ijim.v11i6.6379

[8] Gikundi, D. (2017). A Mobile application for locating the available handyman services within a locality.

[9] Kasamani, B. S., & Gikundi, D. (2017). A Location-Based Service for Handyman Order Placement. Journal of Systems Integration, 8(4), 29–41. https://doi.org/10.20470/jsi.v8i4.309

[10] Ullah, F., Sepasgozar, S., & Ali, T. H. (2019). Real Estate Stakeholders Technology Acceptance Model (RESTAM): User-focused Big9 Disruptive Technologies for Smart Real Estate Management. International Conference on Sustainable Development in Civil Engineering, December 1–8. https://www.researchgate.net/publication/337772796

[11] Walmsley, A. P., & Kersten, T. P. (2020). The imperial cathedral in Königslutter (Germany) as an immersive experience in virtual reality with integrated 360° panoramic photography. Applied Sciences (Switzerland), 10(4). https://doi.org/10.3390/app10041517

[12] Kim, H., Kwon, Y., & Choi, Y. (2020). Assessing the impact of public rental housing on the housing prices in proximity: Based on the regional and local level of price prediction models using long short-term memory (LSTM).Sustainability(Switzerland),12(18).https://doi.org/10.3390/su12187520

[13] Ariyawansa, R. G. (2020). Is COVID -19 a Challenge or an Opportunity for the Real Estate Market and Economy of Sri Lanka? December 1–11.

[14] [14] Ruzaik, F., & Begum, M. (2021). Socio-Economic Challenges of COVID-19 in Sri Lanka. International Journal of Scientific and Research Publications (IJSRP),11(2),185–194. https://doi.org/10.29322/ijsrp.11.02.2021.p11021

[15] Phadnis R, Wickramasinghe C, Zevallos JC, Davlin S, Kumarapeli V, Lea V, et al. (2021) Leveraging mobile phone surveys during the COVID-19 pandemic in Ecuador and Sri Lanka: Methods, timeline and findings. PLoSONE16(4):e0250171.https://doi.org/10.1371/journal.pone.0250171.

[16] "Landlord-Tenant Relationship Amid Covid-19" [Online]. Available: https://www.capitallawchambers.com/covid-19/landlord-tenant-relationship-amid-covid-19/ [Accessed: Sep 12, 2021]

[17] "Sri Lanka rents falling on expat exit, Covid-19 but low rates help real estate buys [Online]. Available: https://economynext.com/sri-lanka-rents-falling-on-expat-exit-covid-19-but-low-rates-help-real-estate-buys-75179/ [Accessed: Sep 17, 2021]

[18] "COVID-19 reshaping the Sri Lankan Real Estate Market: Impact & Outlook" [Online]. Available: https://economynext.com/sri-lanka-rents-falling-on-expat-exit-covid-19-but-low-rates-help-real-estate-buys-75179/ [Accessed: Sep 21, 2021]

[19] "How Has COVID 19 Impacted The Real Estate Market In Sri Lanka" [Online]. Available: https://www.homelandsskyline.lk/how-has-covid-19-impacted-the-real-estate-market-in-sri-lanka/ [Accessed: Sep 10, 2021]

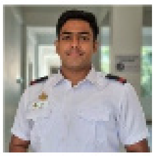
[20] "Top 10+ Real Estate App Development Companies in Sri Lanka — Real Estate App Developers Sri Lanka September 2021" [Online]. Available: https://topsoftwarecompanies.co/real-estate/app-development/agencies/sri-lanka [Accessed: Sep 24, 2021]

ACKNOWLEDGMENT

The completion of the undertaking could not have been possible without the participation and assistance of so many people whose names may not all be enumerated. Their contributions are sincerely appreciated and gratefully acknowledge. However, the authors would like to express their deep appreciation and indebtedness particularly to Mrs. Dinoo Gunasekera for her support and encouragement. Her dynamism, vision, sincerity, and motivation have deeply inspired us. It was a great opportunity and honor to do this research under their guidance. Finally, be thankful for everyone who helped to succeed this.

AUTHOR BIOGRAPHY/IES

MTA Wickramasinghe is a 4^{th} year Information Technology Undergraduate of Faculty of Computing, General Sir John Kotelawala Defence University.



SHIDN de Silva is a 3^{rd} year Information Technology Undergraduate of Faculty of Computing, General Sir John Kotelawala Defence University.

Mrs. D Gunasekera is currently Lecturer (Probationary) at Department of Information Technology, Faculty of Computing at General Sir John Kotelawala Defence University.

Date of publication July 31, 2022, date of current version Aug. 12, 2022.

A Conceptual Architecture for Monitoring Students in Zoom during Online Educational Sessions

PKSC Jayasinghe [1#], EHMPMWijerathna [1], and SY Rajapaksha[2]

[1]Department of Information and Communication Technology, Faculty of Technology, University of Ruhuna, Sri Lanka.
[2]School of IT and Computing, Sri Lanka Technological Campus, Ingiriya Road, Padukka. Sri Lanka.
[1#]subash@ictec.ruh.ac.lk

ABSTRACT Recently the education systems around the world have adhered to a distance learning/teaching method. However, this approach don't provide any guarantee that participated students are presented during the session. The given solution is suggested as an add-on feature in Zoom. This feature enables the teacher to detect the students' availability. The main objective of the architecture is to check the availability of students in the meeting time to time. In this architecture automatic image capturing and processing techniques are used. According to the proposed method images of students are captured automatically and periodically to a previously defined time interval. This is done by manipulating the camera in Android and making the preview of the camera invisible. The captured images are sent to the Zoom cloud to identify the identity of the student. Previously created image vectors (during training period) of students will be there to do the comparisons. Technologies like face embedding, Artificial Neural Network (ANN) are used in identification process of image processing. If they are proven to be the legit participants, the students are accepted to the meeting from the waiting room. Periodically captured images are sent to the face detection by image processing using technologies as Viola Jones algorithm, Haar-like Features, AdaBoost algorithm, Cascading Classifiers, OpenCV. If the student is not available in the seat, a message is sent to the teacher. Even though this conceptual architecture has few limitations, this will be a great help in detecting the students' identities and availability during learning/teaching environment.

INDEX TERMS: AI, Conceptual Architecture, Image Processing, Online sessions.

I INTRODUCTION

A *Background*

The world is evolving day by day and man with it. People are living in a technological era where technology is integrated into every field in human life. For health care, education, business field, and other day to day chores, technology has become an essential resource. The necessity of technology incorporation has become an inevitable change due to the current situation in the world. COVID -19 has changed the world's way into a new norm by reducing the human contact in the society. Especially the education systems all around the world have adhered to a distance learning/teaching method. As a result of that, education in all over the world has changed dramatically, with the distinctive rise of e-learning, whereby teaching and learning are undertaken remotely and on digital platforms.

In this situation online communication platforms as Zoom, MS Teams, Skype and Google Meet have become popular and has widely used by almost every country around the world. The mobile devices and laptops have become the new educational facilitator for most of the students and teachers in this new norm. Out of the wide range operating systems, Android is the most popular at present as exemplifies in Figure 1. When it comes to the global smartphone market, the Android operating system dominates the competition. According to Statista, in 2019 Android had an 87 percent share of the global market, while Apple's iOS had only 13 percent. This gap is expected to increase over the next few years [1]. Furthermore, Web analytics firm StatCounter reported that, for the first time ever, Android topped the worldwide OS internet usage market share. In March 2021, looking at combined usage across desktop, laptop, tablet and mobile, Android usage hit 37.93 percent. That was enough to narrowly overtake Windows' 37.91 percent [2]. Additionally, android provide the developers to experiment with its platform by providing the developer options. In a chaotic situation like this all these educational online platforms came as a blessing in disguise. These tools are used as the main lesson delivery method all around the world. These platforms have some social, technical and pedagogical drawbacks. According to the various researches done previously, there are some concerns that come with online learning. For instance, there are several issues on the internet bandwidth, internet connection, lack of human interaction, disturbances coming from home environment, students not communicating during the virtual classes, teachers' not being able to track the students improvement or engagement in class and not being able to cope up with the technologies are some of them [3], [4], [5].

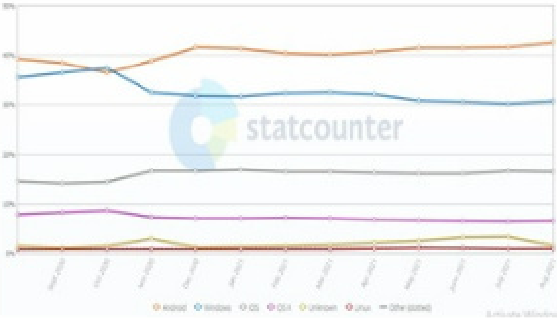


Figure 1. Desktop, Mobile and Tablet OS market share worldwide
Source: Global Statistics (Aug 2020- Aug 2021)

Out of those issues, this research focuses on one technical drawback that teachers/lecturers are facing due to the digitalization of physical classes. As many students had often choose to leave their cameras off [6], it is hard for the lecturers/teachers to find whether the students are presented on the other side or not. However not pressurizing students to turn on their camera is considered as the best student-centered policy during online classroom according to the research done by Costa because some students do not have access to a private space or are embarrassed of their home environment and sometimes they don't have the necessary technical equipment, resources and not being economically feasible to afford flawless internet connection [7]. Therefore considering these both sides (teachers and students), the main objective of this study is to find a technological solution for this issue by making Zoom platform to detect whether the students are actively participating for the session or not by using a combination of several methodologies without making students to turn on their cameras. The Android platform is considered in developing this architecture because as mentioned prior, Android is the widely used platform around the world and the developer freedom in Android is higher than any other platforms.

B Literature Review

In the digital world anything is possible if people know how to manipulate their electronic surrounding properly. Human curiosity and experiments have paved the way for the implement various useful features and apps in technology. In the field of cyber security, the spy wares that are used to spy on people by controlling the device camera is one example for the misuse of knowledge. In 2013 Edward Snowden revealed NSA (National Security Agency) have the ability to watch and spy on users by their laptop/desktop or phone camera at any time, without even having approval or knowledge of the user. Likewise there have being many incidents where hackers has used these spywares to automatically capture live images and videos of people. This newly found knowledge of accessing the cameras of digital devices has coined a new attack term called "Camfecting" in modern technological world [8]. Recently this feature of manipulating the camera to automatically capture images are being used in several researches in different scenarios. Dong et al. developed automatic image capturing and processing for PetrolWatch [9]. This method use to capture a clear image by an unassisted mobile phone from a moving car by manipulating the camera control of the mobile phone and by using image pre-selection schemes. Furthermore, in the study done by Aldaz et al. exemplifies how to automatically capture image through leveraging the sensor capabilities of Google Glass, where SnapCap enables hands-free digital image capture, and the tagging and transfer of images to a patient's EMR [10].

Bah and Ming proposed a methodology to improve face recognition algorithm for attendance management system as the practical application of the suggested algorithm [11]. The existing computer applications of face recognition is able to detect, identify and verify human faces from an image or video for security, identification and attendance purposes. But still some issues are identified which are affected to the accuracy of the face recognition process. Some identified issues are variations and differences in human face due to different lighting conditions, noises in images, different poses/appearances of the face and scale/resolution changes of the image etc. As a solution for that they suggested a new methodology to increase the overall accuracy of the face recognition system. This proposed method was implemented by using Local Binary Pattern (LBP) algorithm with some advanced image processing techniques such as contrast adjustment, bilateral filter, histogram equalization and image blending. However, this finding is unable to address the issue of occlusion and mask faces in face detection and recognition.

Singh and Goel suggested an improvement for the methods of detecting and recognizing human faces by using digital image processing [12]. The suggested improvements consisted with two phases such as detecting a face and identifying the face as an individual from images. In the first phase, face detection process avoided the objects which are placed quite far as a limitation of that approach. The second phase authenticated the identity of the human face by using unique facial characteristics. The above suggested technique is based on biometric technology combined with digital images processing techniques such as the Eigenface method, Fisherface method and PCA (Principal Component Analysis).

Pandey et al. reported a new method to develop a real time parallel vision system based on human face identification for Home Service Robot (HSR) by using real-time image processing techniques [13]. It is a computer application to identify and verify a person automatically from digital image or a video frame from a video source. This suggested system consisted with different sub-systems based on adaptive skin detector, condensation filter with parallel computing particles, Haar-like classifier and a simple and fast motion predictor for tracking, detecting and identifying a human face. The developed system is only able to detect and recognize limited number of human faces. As a solution for that limitation, the study suggested to create much wider database with larger space for recognizing any number of human faces.

II METHODOLOGY AND EXPERIMENTAL DESIGN

A Suggested System Model

The user (student) identification and detection methodologies are incremental approaches which are used to detect the face of the student and recognize the identity of the student from the captured images by using image capturing process. The inputs for these user identification and detection processes are captured images and the detected result as whether the student is really seated or not for the lecture/session is sent to the lecturer/teacher who is a host for the Zoom meeting as the final output. Basically, this methodology consists with four main sections namely image capturing, model training, user identification and user detection. Figure 2 illustrates the overview of this suggested system model.

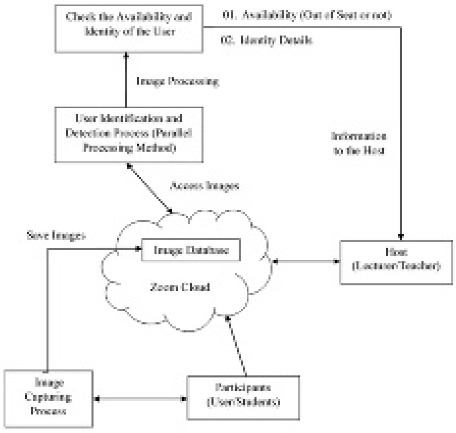

Check the Availability and Identity of the User
01. Availability (Out of Seat or not)
02. Identity Details
Image Processing
User Identification and Detection Process (Parallel Processing Method)
Information to the Host
Access Images
Save Images
Image Database
Zoom Cloud
Host (Lecturer/Teacher)
Image Capturing Process
Participants (User/Students)

Figure 2. Overview of the suggested system model.

Above suggested solution can be added as an add-on to the Zoom tool where it will provide a feature to turn on according to the user's (lecturer/teacher) requirement.

B Training Process

As the initial step of this proposed methodology, training/classifier model should be created. The multiple images of students' faces are used as the training dataset for this classifier model. As the method of taking images of the individual student, in the initial Zoom meeting minimum 50 images of the student should be captured automatically by using image capturing process which is discussed in the section 2.3 in this paper, with every two minutes time gap.

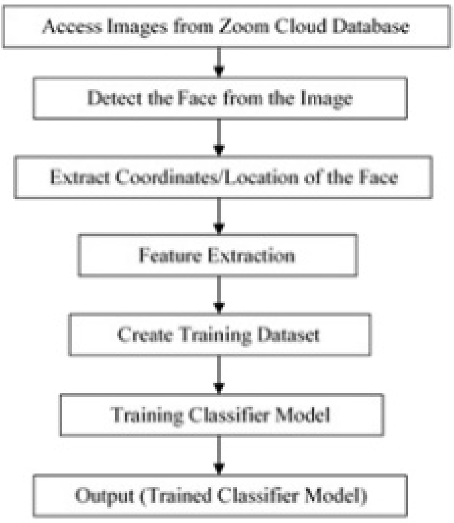

Access Images from Zoom Cloud Database
Detect the Face from the Image
Extract Coordinates/Location of the Face
Feature Extraction
Create Training Dataset
Training Classifier Model
Output (Trained Classifier Model)

Figure 3. Overview of the training process.

There should be minimum 50 images per student to increase the accuracy of the training model and increasing the number of images per student (increasing the training dataset) can be able to get the highest accuracy from the training model. The above captured images of the students are stored in the Zoom cloud database as separate folders for individuals for the training model. These images are accessed as the input training image dataset for the classifier model. Figure 3 illustrates the main steps of this training process.

As the first step of the training process, student's face should be detected from the image. This suggested face detection methodology is discussed in section E in this paper. Then the exact locations/coordinates of the detected face are identified and the face is extracted/cropped by using these identified locations/coordinates. The features are extracted out of the cropped face as the feature extraction process and a pre-trained neural network is used to extract these features. An image of the student's cropped face is taken as an input for this neural network and it outputs a vector which represents the most important features of a face. According to the machine learning, this feature vector is called as face embedding [14]. The dlib and the face_recognition libraries in OpenCV are pre-trained neural network libraries and these libraries contain implementation of deep learning which are used to construct face embeddings (feature vectors) for training and the actual identification process [14].

An Artificial Neural Network (ANN) is used to train this suggested classifier model. An input dataset of this ANN classifier model is created by using above extracted face embeddings (feature vectors). The keras and tensorflow libraries and sequential keras model with dense type keras layers are used for creating this Artificial Neural Network [15]. There is an input layer, hidden layers with several neurons per each hidden layer and output layer. The number of hidden layers and the number of neurons per each hidden layer can be vary according to the input dataset. The output layer consists with several nodes for the expected output values and any specific or auto-generated indexes can be assigned as these expected output values for the students. After successful training of this classifier model, it is stored in Zoom cloud to use in the identification process of the participant (student).

C Image Capturing Process

The first step of the procedure is to capture the photo automatically of the person and then to send it to the image processing to clarify the identity and availability of the person in front of the camera. Therefore the camera should be able to capture a photo of the student automatically according to a given timeline. The best method would be not changing the current functions of the inbuilt camera of the system because it can cause security issues. The study suggests to include a camera as an element of Zoom app. This camera can be given a user-preferred install option while installing Zoom because this is only needed by students rather than the other users of Zoom. The overall process of the image capturing is illustrated by using Figure 4. (In here, an assumption should be made as the Zoom camera is installed during the installation of the Zoom app). The steps given in Figure 4 are further explained as follows.

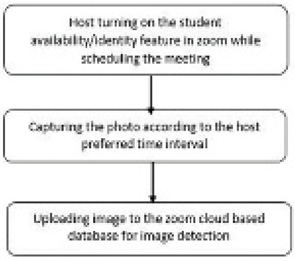

Host turning on the student availability/identity feature in zoom while scheduling the meeting
Capturing the photo according to the host preferred time interval
Uploading image to the zoom cloud based database for image detection

Figure 4. Overview of the image capturing process

1 Giving the permission/turning on the feature to detect students in the other side:

The host or the admin should turn on this feature in Zoom platform when creating the link. This is given as an add-on only in the Zoom platform. When the admin turn on this feature it will be activated to that particular meeting.

2 Capturing a photo according to the given time intervals:

After giving the permission to the process, capturing the image is the initial and the key part of this solution. This is done using the installed Zoom camera of the mobile or the laptop. It is assumed that the permission to access the camera is already given to the Zoom app when installing. The camera of the device (laptop or mobile) captures the photo of the student without their knowledge. The device will not show any preview of the camera to the student. The techniques and technological methods used in spywares to take photos in a legal form. These photos are later sent to the Zoom cloud where the image processing occurs.

Students can use different types of platforms to join a Zoom lecture or a lesson. Some can use laptop while others use mobiles or tabs like devices. Therefore the Operating System (OS) should be compatible with the proposed solution. Given below are the analysis of capturing the photo according to the three different OS platforms. The considered platforms are Windows, IOS and Android.

In Android it is possible to capture a photo without a preview and without disturbing the student. There are various developer options to control the camera in Android. There are numerous apps that has put this mechanism into practice where they are capturing a photo without a preview (for example: "quick camera" app, "Mobile hidden camera" apps). That same method of manipulating the camera can be done in a legal manner with Android since this is given as an embedded feature in Zoom. However in this method, because it is developed as a legally accepted feature, the student should have given camera access permission to Zoom when installing the Zoom app's camera.

Therefore out of these three platforms, Android platform is considered in developing this solution as Android devices are used often by students and it is possible to build the solution with the help of Android developer option. Android provides full access to the device camera hardware. The camera control methods are one of these developer privileges that it provides for the developers. In this scenario, when capturing the image of the student, the preview of the camsera should be invisible or should be hard to glimpse. In Android this can be done by manipulating the camera object and the preview class. The setVisibility() function in startPreview() function, can be set as this.setVisibility(INVISIBLE) to make the surface invisible as soon as it is created or the preview size can be set to 1x1 px, which will make the preview hard to detect. By following these types of camera control methods given by Android in the camera class, the image can be captured without alarming the student on the other side.

Another important feature of this part is the time intervals that photos are captures. The time intervals are configured as random times schedules (the minimum gap between the photo capture is five minutes) and the host is able to choose his/her preferred time interval. The reason for going for a random time intervals is due to the limitation that it has in windows camera access. In windows when accessing the camera the LED is turned on. If it is configured for fixed intervals the student will be able to understand the pattern. Therefore in order to reduce the impact of that limitation the random intervals for image capturing is decided. The minimum gap between two image captures is set to five minutes to give enough time to upload the photo into cloud and to conduct the image processing. Setting a timer to the camera in Android can be implemented by the handler class in java. Image resolution is a crucial factor when it comes to the image processing. The resolution of the photo should be a constant, however the resolution can be changed because of the different qualities of the inbuilt cameras of the devices. Therefore after the photo is captured it is converted in to a common resolution which is the minimum quality that is needed for image processing.

3 Sending it to image processing to clarify the identity:

After capturing the image according to the given intervals, that image is sent/uploaded to the Zoom cloud where the image processing taking place. Along with the captured image of the participant the device identification is sent. The device identification (device name/email name that the profile is created/ profile name, MAC address) is captured and sent along with that particular participant's image. This is done in each and every Zoom meeting sessions. By sending the device identification, it will help the system to understand whom should be accepted and whom should be rejected after the participant identification results arrived. When uploading the image for the image processing, the crucial feature would be the image quality and size. In order for image processing mechanism to work effectively the photo will be set to a common size and a common quality.

D User Identification Process

User identification is the process of recognizing the identity of the participant (student) as actually the real student or any other person participates the lecture/session. This process is more important in commercial education like tuition because lecturer/teacher is able to identify the actual identity of the students to give permission only to the authorized students.

While the students are joining the session through Zoom tool, the images are automatically captured. This image capturing process is further explained in section C in this paper. These captured images with respective device identity details of the students are sent to perform the suggested identification process. The above mentioned device identity details are valid only for the particular Zoom session and these details should be sent along with the captured image in every login to the session. Then by using this suggested identification approach, the students are identified and their identity details are sent with the respective device identity details to the Zoom for the acceptance of their login to the session. If there is a mismatch of the detected identity with the real identity of the students, then they are kept in the waiting room without giving access to join the session. If the student's identification details are correct, then they would be able to join the session as a legit participant. This suggested identification methodology should be processed as parallel processing because the images of all the students of the class should be processed at same time for identification purpose [16]. Figure 5 illustrates the main steps of this proposed identification approach.

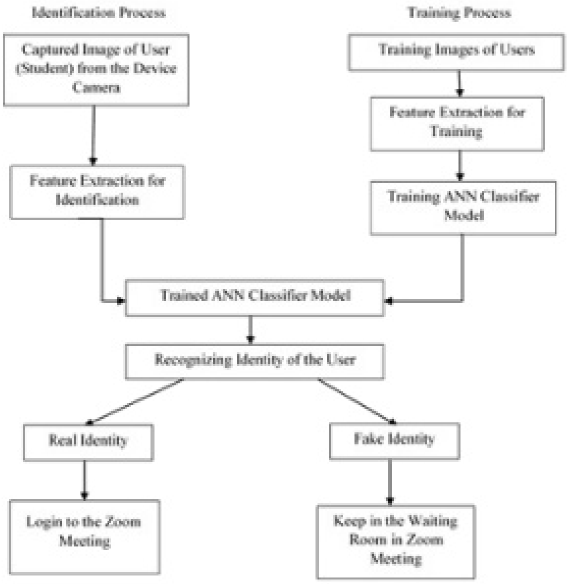

Identification Process
Training Process
Captured Image of User (Student) from the Device Camera
Training Images of Users
Feature Extraction for Training
Feature Extraction for Identification
Training ANN Classifier Model
Trained ANN Classifier Model
Recognizing Identity of the User
Real Identity
Fake Identity
Login to the Zoom Meeting
Keep in the Waiting Room in Zoom Meeting

Figure 5. Overview of the User Identification Process.

As the first step of this identification process, when student is joined the zoom meeting, an image is captured automatically and student's face is detected by using that captured image. The suggested face detection methodology is discussed descriptively in section E in this paper. Finally, with the use of detected face of the student, it is successfully recognize whether the student's identity is real or fake which is the final outcome of this approach.

E User Detection Process

User detection is the process to clarify about the presence or the absence of the participant (student) for a long time period from the lecture/session. For this proposed detection methodology, the images of the students are randomly captured during the Zoom meeting. This image capturing process is discussed in section C in this paper. This suggested detection approach should be processed as parallel processing method because these captured images of all students in the class should be processed as parallel to detect the availability of the students during the Zoom meeting [16].

The captured images of the student are pre-processed as the first step and these pre-processed images are used to extract features and all of these extracted features are not useful and important. Therefore extracted features should be optimized for the classification process. If there is a face on the images, it can be detected as the output from this process. If the face is not detected as the outcome, then a message is sent with the identity details of the student to the host (lecturer/teacher) in the zoom meeting to notify about the absence of the relevant student. This suggested user detection process is used the Viola Jones algorithm, AdaBoost algorithm and cascading classifiers to determine whether there is any face in an image or not [17]. This process can be further subdivided as extracting features of the face, optimizing extracted features and classification process. Figure 6 illustrates the main steps of this approach.

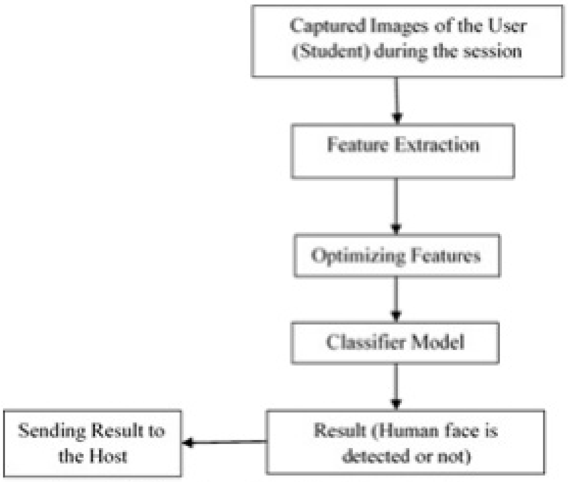

Captured Images of the User (Student) during the session
Feature Extraction
Optimizing Features
Classifier Model
Result (Human face is detected or not)
Sending Result to the Host

Figure 6. Overview of the User Detection Process.

1 Extracting features of the face:

Before go through the feature extraction process, image should be converted to a grayscale format by using cvtColor() function in OpenCV as the image pre-processing [18] because it can simplify the complexity of the image and it leads the way to achieve more effective results. In addition to that it can increase the speed of the image processing.

After image pre-processing, the Viola Jones algorithm is used to continue the feature extraction process. This algorithm is used Haar-like features which are called as digital image features to detect a face by looking at many smaller sub regions of the image for some specific features. All human faces have some universal properties like eyes region, nose region etc. The lightness and the darkness of pixels in the regions are used to recognize these unique properties in the human face. The sum of the pixel values is used to identify the regions as summation value of darker region is smaller than the summation value of lighter region. When it is dealing with large features, these computations can be very complex and it needs to be performed for each feature. As a solution for this problem, integral images are used to perform these computations quickly. Then by using this process, features of the image can be extracted for the optimizing process [17].

2 Optimizing extracted features:

There are different sizes of detector windows which are used to find and match the face in the image by using above extracted features. The one popular detector window is 24x24 detector window which has nearly 160000 number of features available. But there are only a few of these features which are important to identify a face. The AdaBoost algorithm which is a machine learning algorithm for identifying the best features among the huge number of features, is used to optimize these 160000 number of features in to around the best and the important 2500 features for detecting a face [17].

3 Classification process:

The above mentioned 24x24 detector window is used to slide over the image to detect whether any region contains a face or not. Also the cascading classifiers are used to discard non-faces, and avoid wasting time and computations. This cascading classifiers are used to divide the process of detecting a face into multiple stages. The best features such as eye region, nose region etc. are used for the first stage classifier and all the other remaining features are used for the next stages as second stage classifier, third stage classifier etc. When an image sub region enters the cascading classifiers, the first stage is evaluated for identifying its features and if it gets result as positive, meaning that it thinks it can be a face and the output of the stage is, "it may be a face". When a sub region gets that result, it is sent to the next stage of the classifiers and the process continues until it reach the last stage. If all the classifiers give positive output, then it is classified as a human face and if any stage from beginning to last gives negative output then image is immediately discarded since it is detected not as a human face [17].

OpenCV comes with a lot of pre-trained Haar cascade classifiers such as classifiers for smile, eyes, face, etc. For making this detection process simple and easy, these pre-trained Haar cascade classifiers also can be used along with the CascadeClassifier() function. detectMultiscale module of the classifier can be used to detect the face and it can return coordinates of the detected face as output [18]. Finally it is able to detect the student's face from the image with the coordinates as the result from this approach.

III RESULTS AND DISCUSSION

The main objective of this proposed architecture is to detect the presence or the absence and the real identity of the participant (student) on other side. As the result of the image capturing process, the images of the students are successfully captured without disturbing them. As the output of the detection approach, the host (teacher/lecturer) is able to detect whether the students are participating for the session or not without making them to turn on their device camera. It is more flexible way for both sides (teachers and students) and it can improve the efficiency and activeness of both online teaching and learning. As the outcome of the identification approach, the real identity of the student is successfully detected. Moreover, this approach is very useful and effective in commercial education like tuition because lecturer/teacher is able to give permission only to the authorized students.

Given below are two test cases for a valid user (participant A) and an invalid user (participant B) respectively to further explain the above summary of the results.

A Test case for participant A (valid) and B (invalid)

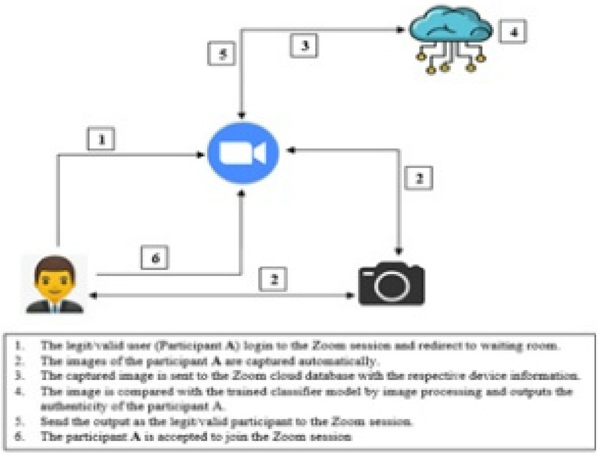
1 Identification Process for Participant A (Figure 7) and B (Figure 9):

The participant A, who is a legit/valid participant for the particular online educational session, is logged to the Zoom meeting. The participant B who is not a legit participant for the particular class is also logged into the Zoom session. After logging in, all the participants are kept in the waiting room for the identification process. While participant A and B are in the waiting room, images of both participants are automatically captured. This captured images of the participant A and B are then sent to the Zoom cloud database with the device identification details of each, to perform the identification process. During this process, trained classifier model compares the features of the captured image of the participant A and give the result as the detected identity is matched with the real identity. Then the participant A is considered as a legit/valid participant for the session. The device identification details of the participant A along with his identity details are sent to the Zoom for the acceptance of the login. As the final step of this approach, the participant A is able to join the session as a legit/valid participant.

While for the participant B, the comparison done by the classifier model decides that participant B is not a legit participant for this class. That result is then sent to the Zoom along with the device identification of the participant B. Since it will be given as an unauthorized participant, the participant B is not admitted to the Zoom session. Hence, he is kept in the waiting room.

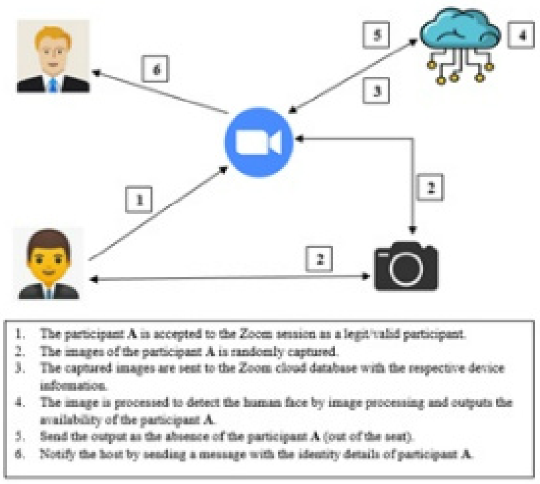
2 Detection Process for Participant A (Figure 8):

After performing the identification process, the participant A is accepted to the online session as an authorized participant. The images of the participant A are randomly taken during the Zoom meeting. The above captured images are sent to the Zoom cloud database for the detecting process to verify the presence or the absence of the participant A in time to time. In detection approach, the above captured image is processed to detect the human face on it as the final outcome. If the participant A is not in the seat, it is recognized by the detection process and notify the host (teacher/lecturer) by sending a message with his identity details. Then the host is able to detect the absence of the participant A.



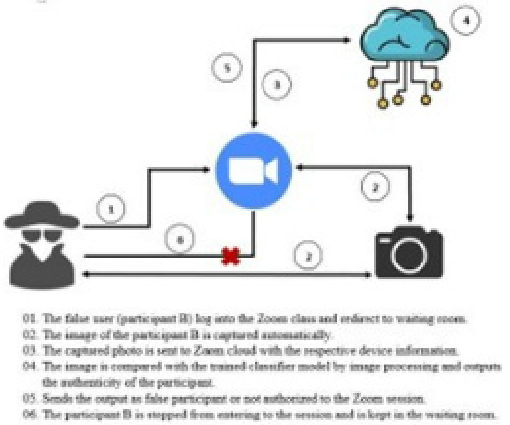
1. The legit/valid user (Participant A) login to the Zoom session and redirect to waiting room.
2. The images of the participant A are captured automatically.
3. The captured image is sent to the Zoom cloud database with the respective device information.
4. The image is compared with the trained classifier model by image processing and outputs the authenticity of the participant A.
5. Send the output as the legit/valid participant to the Zoom session.
6. The participant A is accepted to join the Zoom session

Figure 7. Valid participant A – Identification process



1. The participant A is accepted to the Zoom session as a legit/valid participant.
2. The images of the participant A is randomly captured.
3. The captured images are sent to the Zoom cloud database with the respective device information.
4. The image is processed to detect the human face by image processing and outputs the availability of the participant A.
5. Send the output as the absence of the participant A (out of the seat).
6. Notify the host by sending a message with the identity details of participant A.

Figure 8. Valid participant A – Detection process.



01. The false user (participant B) log into the Zoom class and redirect to waiting room.
02. The image of the participant B is captured automatically.
03. The captured photo is sent to Zoom cloud with the respective device information.
04. The image is compared with the trained classifier model by image processing and outputs the authenticity of the participant.
05. Sends the output as false participant or not authorized to the Zoom session.
06. The participant B is stopped from entering to the session and is kept in the waiting room.

Figure 9. Invalid participant B – Identification process.

Even though in this framework is considering only Android OS, the covert image capturing can be implemented for Windows and IOS as well. For example in windows the camera of the laptop can be accessed through manipulating firmware/BIOS of the system. However, since this is proposed as an inbuilt feature for Zoom, accessing the camera illegally won't be necessary. The only issue in accessing the camera in Windows platform is the LED bulb that is embedded in the laptop. The light also can be turned off as some spyware software does, however if the camera light is connected by a hardware mechanism it is hard to turn off the light while capturing the photo. In that case the random photo capturing intervals will be a blessing in disguise, because even though it is complex than static time intervals, it will stop from making students to find out about the pattern of photo capturing.

Implementing this architecture in Mac OS is slightly challenging than the other two operating systems. However it is not impossible as there are apps that are used to take covert images of others using IPhone's inbuilt camera like "SneakyPix" app. Nevertheless, for this operating system also the student should have given the camera access permission to Zoom as it is coming as a default feature in Zoom.

IV CONCLUSION

This study propose a conceptual architecture to monitor whether the students are participating for the session or not and the real identity of students without forcing them to turn on their camera. It is suggested as an add-on to the Zoom tool where it will provide a feature to turn on according to the user's (teacher) requirement. Since the user detection and identification processes occur concurrently during session the processing time can be high. Therefore, as a solution for that issue, parallel processing techniques are suggested. According to the study, it is only discussed on Android OS platform but there is a scope to carry out further research on implementing it in other different OS platforms like Windows and Mac can be implemented as further works.

Nowadays the online communication platforms such as Zoom, MS Teams, Skype and Google Meet have become popular and are widely used by almost every country around the world. The proposed architecture provide solution only for Zoom platform. However, other different online communication platforms can also be implemented according to this proposed architecture.

This proposed architecture will assure the fact that students will not boycott the educational sessions even though it is in a virtual platform. It will make the online education to go one step forward in adopting the effectiveness of a physical classroom. The students' availability will be monitored even their cameras' are turned off which will give the upper hand to the host of the educational session. It will allow students to learn efficiently as they are learning in a physical classroom.

Additionally, this solution will be an advantageous movement for online exam proctoring and for private tuition classes because of the proposed identification process of the participants. The invigilator or the teacher will be able to identify the authenticity of the logged in student with this Zoom add on. With the current situation in the world, the online/virtual education will be the only solution to conduct the lessons. Therefore it is an utmost necessity to identify the issues in virtual education and to propose solutions for them to make it more effective.

REFERENCES

[1] J. Cohen, IOS More Popular in Japan and US, Android Dominates in China and India, Available: https://www.pcmag.com/news/ios-more-popular-in-japan-and-us-android-dominates-in-china-and-india, 2020, Accessed: 03 August 2021.

[2] M. Smith, Privacy and security fanatic, CSO, Available: https://www.csoonline.com/article/3187011/android-is-now-the-worlds-most-popular-operating-system.html, 2017, Accessed: 03 August 2021.

[3] V. Saminathan, Problems of online classes, International Journal of Academic Research Reflector, vol. 9, pp. 1-3, 2020, DOI: 10.6084/m9.figshare.13573550.

[4] A. Ullah, M. Ashraf, S. Ashraf and S. Ahmed, Challenges of online learning during the COVID-19 pandemic encountered by students in Pakistan, Journal of Pedagogical Sociology and Psychology vol. 3(1), pp. 36-44, 2021, DOI: http://www.doi.org/10.33902/JPSP.2021167264.

[5] M. Mahyoob, Challenges of e-Learning during the COVID-19 Pandemic Experienced by EFL Learners, Arab World English Journal (AWEJ), vol. 11(4), pp. 351-362, 2020, DOI: https://dx.doi.org/10.24093/awej/vol11no4.23.

[6] F. R. Castelli, M. A. Sarvary, Why students do not turn on their video cameras during online classes and an equitable and inclusive plan to encourage them to do so, Academic practice in ecology and evolution, vol. 11(8), pp. 3565-3576, 2021, DOI: https://doi.org/10.1002/ece3.7123.

[7] K. Costa, Cameras be damned, Available: https://www.linkedin.com/pulse/cameras-damned-karen-costa/, 2020, Accessed: 04 August 2021

[8] A. Sommacal, Camfecting: what it is and how we can protect ourselves from it, UNIlab blog, Available: https://www.unilab.eu/articles/coffee-break/camfecting/, 2018, Accessed: 07 August 2021.

[9] Y. Dong, S. Kanhere, C. T. Chou, and R. Liu, Automatic image capturing and processing for PetrolWatch, Proceedings of the ICON 2011 - 17th IEEE International Conference on Networks, pp. 236-240, 2011, DOI: 10.1109/ICON.2011.6168481.

[10] G. Aldaz, L.A. Shluzas, D. Pickham, O. Eris, J. Sadler, S. Joshi and L. Leifer, Hands-free image capture, data tagging and transfer using google glass: a pilot study for improved wound care management, Plos One vol. 10(4), 2015, DOI: https://doi.org/10.1371/journal.pone.0121179.

[11] S.M. Bah, F. Ming, An improved face recognition algorithm and its application in attendance management system, Array, vol. 5 (100014), 2020, DOI: https://doi.org/10.1016/j.array.2019.100014.

[12] G. Singh, A.K. Goel, Face Detection and Recognition System using Digital Image Processing, 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 348-352, 2020, DOI: 10.1109/ICIMIA48430.2020.9074838.

[13] K. Pandey, R. Lilani, P. Naik, G. Pol, Human Face Recognition Using Image Processing, International Journal of Engineering Research and Technology (IJERT) vol. 2(04), 2014.

[14] H. Mujtaba, Face Recognition with Python and OpenCV, Available: https://www.mygreatlearning.com/blog/face-recognition/, 2021, Accessed: 05 August 2021.

[15] P. Wijerathna, L. Ranathunga, Rice Category Identification using Heuristic Feature Guided Machine Vision Approach, IEEE 13th International Conference on Industrial and Information Systems (ICIIS 2018), pp. 185-190, 2018, DOI: https://doi.org/10.1109/ICIINFS.2018.8721396.

[16] S. Yalamanchili, J.K. Aggarwal, Parallel Processing Methodologies for Image Processing and Computer Vision, Advances in Electronics and Electron Physics, vol. 87, pp. 259-300, 1993, DOI: https://doi.org/10.1016/S0065-2539(08)60018-9 .

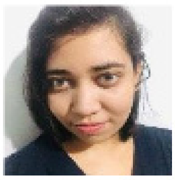
[17] H. Mujtaba, Face Detection using Viola Jones Algorithm, Available: https://www.mygreatlearning.com/blog/viola-jones-algorithm/?highlight=face

[18] P. Pandey, Face Detection with Python using OpenCV, Available: https://www.datacamp.com/community/tutorials/face-detection-python-opencv, 2018, Accessed: 02 August 2021.

AUTHOR BIOGRAPHIES

Dr. P.K.S.C. Jayasinghe attached to the Department of ICT, Faculty of Technology, University of Ruhuna. Presently he serve as the head of the department. He has number of research pub-lications in both journals and symposiums related to IT domain.

E.H.M.P.M.Wijerathna attached to the department of ICT, Faculty of Technology, University of Ruhuna as the lecturer. Her main research interest is image processing. She has several research publications on this field.



S. Y. Rajapaksha works as the lec-ture in School of IT and Computing, Sri Lanka Technological Campus. She worked in Department of ICT, Faculty of Technology, University of Ruhuna as a temporary lecturer. She graduated in SLIIT specializing in Cyber security. She has several publications related to the Cyber security.

Printed at KDU PRESS
General Sir John Kotelawala Defence University
Kandawala Road
Rathmalana
Sri Lanka

ISSN 2820-2147
9 772820 214004