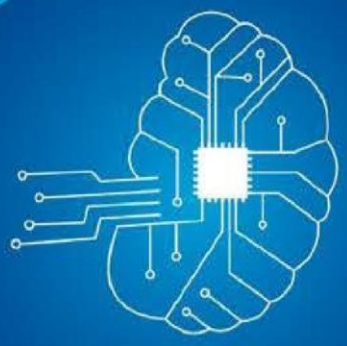
NEAR EAST UNIVERSITY

JOURNAL FOR ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS

Volume: 4 Issue: 2

ISSN: 3062-1968



www.neu.edu.tr

JOURNAL OF ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS
Uluslararası, Hakemli Dergi / International, Refereed Journal

May, 2025
Cilt-Volume 04/ Sayı-Issue 02

Foundation Year of the Journal
2022

Publication Contact

Editorial Board
editor.aiit@neu.edu.tr

Contact for Information

info.aiit@neu.edu.tr

Address and Contact

Near East University Innovation and Information Technologies Centre International Research Center for AI and IoT Yakın Doğu Bulvarı, PK: 99138Lefkoşa / TRNC, Mersin 10 – Türkiye Phone:+90 (392) 223 64 64/+90 (392) 680 20 00
Faks:+90 (392) 223 64 61

http://dergi.neu.edu.tr/ https://iot.neu.edu.tr/

CONTENTS

Evaluation Of Factors That Increase The Morale Of Teachers: What Is The Impact Of Artificial Intelligence And New Technologies In Teaching

Canan Konat, Fahriye Altınay, Gökmen Dağlı, Zehra Altınay

[1] *Ministry of Education, canankonat17@gmail.com*
[2] *Faculty of Education, Near East University fahriye.altinay@neu.edu.tr*
[3] *Faculty of Education, University of Kyrenia, gokmen.dagli@kyrenia.edu.tr*
[4] *Faculty of Education, Near East University zehra.altinaygazi@neu.edu.tr*

ABSTRACT

Expectations from teachers in society are constantly changing and evolving. In order to respond to these expectations, teachers are constantly changing and developing. At this point, morale lies behind the continuous development of teachers. This study aimed to determine moraleboosting factors such as using articial intelligence and new technologies within the framework of teachers' low and high morale symptoms. For this purpose, semi-structured interview questions were prepared to obtain data. The prepared questions were finalized by taking expert opinion. The study group of the research was determined on a voluntary basis from the selected teachers in TRNC Primary schools. The collected data were divided into themes and codes and content analysis was performed. As a result of the research, factors that reduce and increase teacher motivation were identified. It has been determined that the first thing that increases teacher morale is that teachers have good relationships with each other. The scarcity of studies in the field of moral motivation in education in our country increases the importance of the results obtained from this research.

KeyWords: *Artifical Intelligence, Morale, Motivation, New tecnologies*

1. INTRODUCTION

Nowadays, everything is in a constant state of development and change. Technology is changing rapidly and society is having a hard time keeping up. Developing technology also greatly affects the psychosocial development of children. We, as adults, have a hard time attracting children's attention during this period. Even children's playing habits have changed. Now, instead of playing with their friends in the park or garden as before, they prefer various technological devices such as smartphones, computers and tablets. This situation is also reflected in the school. It becomes very difficult to attract the child's attention and interest to the lesson. Teachers, who are the most important element of our society, have a great responsibility. Expectations from teachers in society are constantly changing and evolving. In order to respond to these expectations, teachers are constantly changing and developing. At this point, morale lies behind the efficiency of teachers. Having well-equipped teachers is an important factor in student success. Teachers' morale levels are at least as important. It is observed that teachers with high morale levels have a positive impact on student success (Tanriöğen, 1995).

There are many factors that affect a teacher's morale. Nowadays, using artificial intelligence and news technologies in teaching is also factor to effect motivation and of course morale of the teachers. Some of these factors are the organizational structure of the school, the attitude of administrators towards teachers, working conditions, the level of job satisfaction and the life of teachers outside the school (Eren, 2012). Increasing teacher morale increases student success and efficiency. When we identify the symptoms of low and high teacher morale, it is possible to uncover the problems that cause these symptoms. It can be seen that there are many studies in the literature about the motivation and morale of teachers. Studies have focused on the factors affecting teachers' job satisfaction and motivation. Abazaoğlu and Aztekin (2015) investigated the effect of teacher morale and motivation on students' science and mathematics achievements and revealed that, in general, high teacher motivation in countries positively affects students' academic success. According to Aydin (2011), except for teachers working in private schools; When the morale status of teachers working in primary and secondary schools affiliated with the Ministry of National Education was evaluated by looking at these symptoms, it was seen that the factors indicating low morale were more dominant. Considering that teacher morale has a very important place in the education-training process; He stated that measures should be taken as soon as possible to turn this profile into high morale indicators. He stated that great responsibilities and duties await education administrators at all levels, especially the Ministry of National Education officials. Tanrıöğen (1995) conducted research on teacher morale. He presented a research on teachers' expectations regarding motivation from school administrators and education supervisors. The main problem of the research is: What are the morale-enhancing factors within the framework of low and high morale symptoms of teachers in primary schools? It was determined as .

It is thought that teachers with high morale levels will increase their productivity towards their students. According to the research conducted by Avanoğlu in 2018, a significant relationship emerged between teachers' communication skills and morale. Teachers who establish and maintain healthy communication with their colleagues change the atmosphere in the school, their self-confidence increases, they see themselves as a part of the institution, they are willing to improve themselves, they love teaching and do it with enthusiasm, and they are willing to cooperate. As a result, it is thought that teachers' morale levels have increased. In

their research in 2015, Abazaoğlu and Aztekin found that high teacher motivation positively affected students' academic success in samples from Singapore, Japan, Finland and Turkey. In the research conducted by Başıbüyük in 2012, there are high-level relationships between teacher morale characteristics and job commitment. It is concluded that in organizations where teacher morale is high, their commitment to work will increase. Accordingly, it can also be thought that teacher productivity will increase.

In their research, Ersoy and Başer (2010) found that student motivation varies depending on the student's environment such as school and environment, thus motivation is another factor that affects the student's academic success and ability to solve the problems he encounters. The high morale level of teachers working at the school affects the school climate and, as a result, leads to changes in the academic success of students. According to the research of Tanrıöğren in 1995, teachers with high morale levels are those who enjoy teaching, try to improve themselves personally and professionally, have good relations with the school principal, cooperate with other teachers and have positive thoughts about them, and have positive relationships with their schools. It turns out that they are individuals who are proud of their status, satisfied with the school's facilities and services, the environment and their parents, and have good relations with the students.

The aim of this research is to ensure that teachers can do their jobs with passion, pay individual attention to students, instill positive behaviors in students, ensure that students become more self-confident individuals, know their responsibilities, approach those around them with respect and love, and raise individuals who ask questions, do not accept the situation as it is, but question and investigate, and gain satisfaction from their jobs. they should take it. It is known that this is directly related to their high morale. In this context, it is very important to detect signs of high morale. Increased productivity of administrators, teachers and students is associated with high morale. It is believed that identifying these signs of high morale and taking steps in this direction will bring success in many areas. In line with these explanations, the aim of the study was to determine the morale-boosting factors within the framework of teachers' low and high morale symptoms.

2. METHOD

2.1 Model of the Research

Research method is defined as the tools used to fulfill the qualities and objectives of a research process. There are many methods to achieve a goal and result. When conducting a research, it is of great importance to choose the most appropriate method to achieve the goal effectively. If the research method is chosen correctly, the accuracy and result of the research will be revealed (Açiler, Sezer. 2020).

It seems that the most used research method from past to present is quantitative research. However, since quantitative research results provide general information, they are now less preferred in the fields of philosophy, educational sciences and social sciences. Thanks to qualitative research, more detailed, descriptive and in-depth information can be obtained in fields such as philosophy, educational sciences and social sciences(Açiler, Sezer. 2020).

We can say that qualitative research is a research that clearly reveals the participants' opinions and thoughts on a subject without any limitations by asking open-ended questions. The answers collected are not numerical. It is a research method that tries to reveal views and ideas on a subject rather than finding numerical data on that subject. It allows in-depth research of the subject.

In this study, qualitative research was used to determine the factors that increase the morale of primary school teachers. According to Yıldırım and Şimşek (2018), qualitative research is research in which qualitative data collection methods such as observation, interview, and document analysis are used and a qualitative process is followed to reveal perceptions and events in a realistic and holistic way in a natural environment. In this research, qualitative data collection methods such as observation, interview and document analysis were used. In this research, it was modeled as a case study within the scope of qualitative research method. Since the factors that increase teachers' morale will be examined separately in the research, the research was designed as a multiple case study among case studies.

2.2. Working Group

Teachers who provide education at the primary education level as the working group. While determining the study group of the research, 3 primary schools affiliated to Ministry of National Education were determined. The study group of the research consisted of teachers working in the selected schools and participating on a voluntary basis. It was determined that 20 volunteer teachers from the selected schools would participate in the research.

2.3. Data Collection Tools

In this research, semi-structured interview questions were used as a data collection tool. It was aimed to determine teachers' thoughts about factors that increase their morale. The semistructured interview form was prepared by taking expert opinions. In addition, research data was collected through a personal information form and researcher diary. An attempt was made to increase the validity and reliability of the research by using multiple data sources during the data collection process. **2.4. Collection of Data**

In this study, data were collected with the help of semi-structured interview questions, personal information form and researcher diary developed by the researcher by taking expert opinions. The data of the research was collected from teachers teaching at the primary education level under the TRNC Directorate of National Education. The data was collected from teachers in selected schools on a voluntary basis. In the research, the data were examined separately while determining the factors that increase teachers' morale. Three primary schools affiliated with the TRNC Ministry of National Education were selected to collect research data. Data were collected from 20 volunteer teachers in total.

2.5. Analysis and Interpretation of Data

In this research, data collected through semi-structured interviews were analyzed through inductive analysis. The data was divided into themes and codes and content analysis was performed. Content analysis method, which is among the qualitative data analysis methods, was used to analyze the interview data.

3. FINDINGS AND COMMENTS

This section contains the findings regarding the analyzes made for the research problem. The findings obtained as a result of the research were presented and interpreted in tables under the subheadings opened for each research question.

Findings Related to Research Questions Table 7. Findings Regarding Teachers' Definition of the Concept of Motivation

Participants'	Opinion on Motivation	Percentage
K1	Peaceful and feeling good	%5
K2	Focus on the task at hand	%15
K3	Trying to do the best with endless energy	%5
K4	Meeting expectations	%5
K5	A source of loving what one loves.	%5
K6	willingness to do something	%20
K7	Focus on the task at hand	%15
K8	interest in a job	%5
K9	Focus on the task at hand	%15
K10	willingness to do something	%20
K11	Doing your job peacefully and lovingly	%10
K12	Doing your job peacefully and lovingly	%10
K13	A feeling we must have in order to do a job with the highest efficiency.	%5
K14	willingness to do something	%20
K15	feeling excited to do something	%5
K16	Using energy in the right direction	%5
K17	willingness to do something	%20
K18	The energy required to start and succeed in a business	%5
K19	Instinct that initiates an individual's movements and behaviors	%5
K20	The positive energy we need to do a job happily and excitedly.	%5

As seen in Table 7, teachers' opinions on the definition of the concept of motivation are given. According to the results, the definition of morale was "Willingness to do something" was the most common answer with a rate of 20%. "Focusing on the work done" was given by 15% of the participants. "Doing the job with peace and joy" is the answer given by 10% of the participants. 5% of the participants define the concept of morale as "Peaceful and feeling good", "Trying to do the best with endless energy", "Meeting expectations", "A source of loving the job one loves", "Interest in a job", "A "A feeling we need to have in order to do the job at the highest efficiency", "Feeling excited to do something", "Using energy in the right direction", "The energy required to start a job and be successful in that job", "The instinct that initiates the individual's actions and behaviors" ", “The positive energy we need to do a job happily and excitedly.” He defined it as:

Table 8. Findings Regarding Metaphor Examples of Teachers' Love for Their Profession

Participants'	Metaphor Examples of Love for the Profession	Percentage
K1	Finding sun in cold weather	%5
K2	Like a food I don't like	%5

K3	filial love	%20
K4	Like being cold in hot weather	%5
K5	To grow a seed, turn it into a tree, prepare it for life with its roots and branches, and bear fruit.	%5
K6	cooking with care	%5
K7	Eating a meal I like	%5
K8	It's like shopping with an unlimited card	%5
K9	Growing flowers with care and compassion	%5
K10	It is a sport that I enjoy doing and cannot give up.	%5
K11	Different types of flowers growing in a garden	%5
K12	life adventure	%5
K13	filial love	%20
K14	Like a colorful confetti containing every color	%5
K15	Ingredients that are not delicious on their own come together to create a delicious cake.	%5
K16	Love	%5
K17	Like air, like water. A must have for me!	%5
K18	Just as bees instinctively collect pollen when flowers bloom, I go to school because I feel like it, just like a bee.	%5
K19	filial love	%20
K20	filial love	%20

As seen in Table 8, "Love for children" was the most common answer with a rate of 20% in the metaphor examples of teachers' love for their profession. 5% of the participants said "Cooking with care", "Eating a meal I like", "It is like shopping with an unlimited card", "Growing flowers with interest and affection", "It is a sport that I enjoy doing and cannot give up". "Growing different kinds of flowers in a garden", "The adventure of life", "Like a colorful confetti containing every color", "Ingredients that are not delicious on their own come together to create a delicious cake", "Love", "Like air, water like. It's a must for me!", "Just like bees instinctively collect pollen when flowers bloom, I go to school because I feel like it, just like a bee.", "To find sun in a cold weather.", "It's like a food I don't like.", “It's like being cold in hot weather.”, “Growing a seed, turning it into a tree, preparing it for life with its roots and branches, and bearing fruit.” He gave his answers.

Table 9. Findings Regarding Situations Where Teachers Love Their School

Participants'	Situations Where School Is Loved	Percentage
K1	*Class sizes are not crowded	%45
	*High student motivation	%5
	*Teachers have good relationships with each other	%90
K2	*Teachers have good relationships with each other	%90
	*Class sizes are not crowded	%45
	*The school is close to my home	%50
K3	*It is a small school	%10
	*Teachers have good relationships with each other	%90
	*The school is close to my home	%50

K4	*Class sizes are not crowded	%45
	*Teachers have good relationships with each other	%90
	*The school principal should not be oppressive and should be understanding	%40
K5	*Teachers have good relationships with each other	%90
	*Class sizes are not crowded	%45
	*Assistance in events	%20

K6	*Meeting with teachers outside of school	%20
K7	*Teachers have good relationships with each other	%90
	*Colleagues being collaborative	%15
	*The school principal should not be oppressive and should be understanding	%40
	*Collaboration between teachers	%20
	*Students showing love and respect to teachers	%25
K8	*Teachers have good relations with each other	%90
	*Meeting with teachers outside of school	%20
K9	*It is a small school	%10
	*Teachers have good relations with each other	%90
	*The school is close to my home	%50
	*The school principal should not be oppressive and should be understanding	%40
	* Availability of necessary course materials at school	%15
K10	*Class sizes are not crowded	%45
	*Teachers have good relations with each other	%90
K11	*Teachers have good relationships with each other	%90
	*The school principal should not be oppressive and should be understanding	%40
	*Students showing love and respect to teachers	%25
K12	*Teachers have good relations with each other	%90
	*Assistance in events	%20
K13	*The school principal should not be oppressive and should be understanding	%40
	*The school principal should respect the opinions of the teachers	%10
	*Assistance in events	%20
	*Collaboration between teachers	%20
	*The school is close to my home	%50
K14	*Teachers have good relationships with each other	%90
	*Meeting with teachers outside of school	%20
	*Supporting the school from the parent-teacher association	%5
	*Class sizes are not crowded	%45
	*The school is close to my home	%50

	* Availability of necessary course materials at school	%15
	*Having technological devices in my classroom	%10
K15	*Teachers have good relationships with each other	%90
	* Availability of necessary course materials at school	%15
	*Having technological devices in my classroom	%10
	*The school principal should not be oppressive and should be understanding	%40
	*The school is close to my home	%50
K16	*Students showing love and respect to teachers	%25
	*Teachers have good relationships with each other	%90
	*The school is close to my home	%50
	*The school principal should not be oppressive and should be understanding	%40
	*Teachers have good relations with each other	%90
K17	*Class sizes are not crowded	%45
	*The school is close to my home	%50
K18	*The school principal should respect the opinions of the teachers	%10
	*Parents' respect for teachers	%5
	*Students showing love and respect to teachers	%25
	*Class sizes are not crowded	%45
	*Teachers have good relationships with each other	%90
	*Students' interest in the course	%5
	*The school is close to my home	%50
	*Students enjoy coming to school	%5
K19	*Collaboration between teachers	%20
	*Teachers have good relations with each other	%90
	*Students showing love and respect to teachers	%25
	*Colleagues being collaborative	%15
K20	*Teachers have good relations with each other	%90
	*Class sizes are not crowded	%45
	*The school is close to my home	%50
	*The school principal should not be oppressive and should be understanding	%40
	*Having a peaceful working environment	%5
	*Receiving positive feedback from parents	%5
	*Colleagues being collaborative	%15
	*Collaboration between teachers	%20
	*Meeting with teachers outside of school	%20
	*Collaboration in events	%20

As seen in Table 9, "Teachers' good relations with each other" is one of the most popular reasons for the school, with a rate of 90%. This is followed by "The school is close to my home"

with a rate of 50%. It has been revealed that 45% of teachers like their school if "the number of classes is not crowded". The answer "The school principal should not be oppressive and should be understanding" was said by 40%. The answer "Students show love and respect to teachers" was given by 25%. The answers "There should be cooperation between teachers, meeting with teachers outside the school, cooperation in activities" were given at a rate of 20%. It was determined that the answers "colleagues are sharing, the school has the necessary course materials" were 15%. The answers "The school principal should respect the opinions of the teachers" and "There are technological devices in my classroom" were given at a rate of 10%. "Student motivation is high, the parent-teacher association supports the school, parents respect and show respect to the teacher, students are interested in the lesson, students come to school with pleasure, the working environment is peaceful, and receiving positive feedback from parents" are the answers given by 5%.

4. CONCLUSION AND RECOMMENDATIONS

If we generalize the definition of motivation, we can express it as an individual taking action with an inner desire to do something. Individuals have responsibilities that they must fulfill in their daily lives. They may feel willing or unwilling to do things that fall within these responsibilities. This is where motivation comes into play. An individual with high motivation does not have difficulty in doing this job, has a good time and does his job with pleasure. On the contrary, an individual with low motivation tries to fulfill his responsibilities by forcing himself. Every individual wants to be highly motivated in his daily and working life. It is thought that teachers with high morale will be more productive and open to learning for their students (Tanrıöğen, 1995). High motivation of the teacher enables an efficient education and training process. They can get trainning on how to use new technologies and artificial intelligence for their teaching performance.

Results Regarding Teachers' Definition of the Concept of Motivation; Teachers defined the concept of motivation as follows. In the opinions regarding the definition of morale, the concepts of "peace, focus, energy, love of work, efficiency, willingness, excitement, instinct" came to the fore. Willingness to do something, doing the job with pleasure in peace, feeling peaceful and good, focusing on the job done, trying to do the best with endless energy, meeting expectations, the source of doing the job one loves with love, interest in a job, making a job the best. It is an emotion we need to have in order to do it with high efficiency, it is the energy required to be excited to do something, to use energy in the right direction, to start a job and to be successful in that job, it is the instinct that initiates the individual's movements and behaviors, so that we can do a job happily and excitedly. Definitions have emerged as the positive energy we need. They need further trainning on artifical intelligence and new technologies.

Results of Metaphor Examples of Teachers' Love for Their Profession; Looking at the answers given, 90% of the metaphor examples given by teachers to their love of their profession contain positive expressions, while 10% contain negative expressions. The negative expression here is "It's like eating a food I don't like." and “Like being cold in hot weather.” are the answers. Accordingly, 90% of the participants do their job fondly, and 10% do it without loving their job.

Results Regarding Situations Where Teachers Love Their School; Above are the situations where teachers love the school. The most common answer was that teachers have good

relations with each other. Every individual first wants to establish good, positive relationships with their colleagues. It is accepted that in an organization where the morale level is high, the individual is happy to be in the group he belongs to and his level of commitment to the group is also high (Attitude, 1979; cited in Kırca, 2019). The answer that the school is close to my home is also one of the most frequently given answers. The long distance between the teacher's school and home tires the teacher in many ways. It causes loss of time, money and energy. Crowding of classrooms reduces the teacher's rest time and causes less individual time for each student.

Results Regarding Collaboration and Sharing Experiences Among Teachers; The most important collaboration and sharing experience between teachers was the sharing of lesson notes and annual lesson plans. Teachers share lesson plans with each other in case of class changes or updating their annual plans. Teachers help with exhibition preparations, April 23 events, and reading festival activities. Sharing knowledge, experience and experience between senior teachers and teachers who are new to the profession is also an important sharing experience. Technological information sharing takes place especially between young teachers and senior teachers. It is known that young teachers are more knowledgeable than senior teachers in terms of technological knowledge. Meeting teachers outside of school helps them get to know each other better and share more. It also allows for increased communication.

***Results Regarding Situations That Increase Teachers' Motivation*:** A good teacher environment brings peace. All teachers want the working environment to be a peaceful environment. It has been observed that school principals' respect for teachers' opinions increases motivation. The freedom of the teacher who feels that his opinions are valued and respected will increase, he will put forward new ideas and therefore his productivity will increase. Parents' respect for teachers will make the teacher feel good. When the teacher contacts the parent about any issue, the teacher will not have any reservations. A healthier relationship will be established between teacher and parent. Parents' involvement and giving positive feedback makes the teacher feel that they are not alone in the education process and increases their motivation. It can be seen from the results that the parent factor has an important place among the factors that increase teacher motivation. Seeing students' progress and having high exam scores means that students understand the subject taught. The student's understanding of the subject taught by the teacher makes the teacher feel good and productive. Therefore, the teacher's motivation increases. Education supervisors guide teachers. It is important that the criticisms made by the supervisor to the teacher should be constructive and guiding, not destructive. It is seen that receiving positive feedback and appreciation from the supervisor increases the teacher's motivation.

Results Regarding the Effect of Technology Use on Motivation in the Work Environment and in the Learning and Teaching Process; It was concluded that the use of technology in the work environment and in the learning and teaching process has a positive effect and increases motivation. Nowadays, with the developing technology, it is becoming increasingly difficult to attract the attention of students. Using technology in lessons attracts the student's attention and helps convey the lesson more easily. In this way, some concepts that seem abstract to students become easier to understand and provide great convenience to the teacher. While taking advantage of technological tools provides convenience for every teacher, the lack of this infrastructure in some schools reduces teachers' morale. Teachers who consider themselves inadequate in the use of technological devices are worried about this issue, think that they will fail, and therefore avoid using this method.

Conclusions on the Importance of Having High Motivation in the Work Environment; High motivation in the work environment is important in many respects. When we look at the individual effect of motivation on the teacher, high motivation directly affects factors such as the teacher's energy, peace, efficiency, success, desire for self-improvement, and sense of belonging to the profession. In cases where motivation is low, these factors are also affected. Since we will continue our profession for a lifetime, it is important that our motivation is high. Our motivation is not only neutral to our work, but also to our private lives. Any problems we have in the work environment are reflected in our lives outside of work. In addition, low motivation is reflected in the students in the classroom. The teacher's tolerance decreases. Students are people who are directly affected by teacher motivation. A student always wants to see his teacher smiling.

Suggestions;

- The school principal can provide opportunities for teachers to spend more time with each other and increase their communication by organizing events outside the school.

- In-service training can be provided in the areas of use of technological devices in classrooms and content development. Thus, instead of being afraid of using technology, teachers increase their self-confidence and have the opportunity to improve themselves.

- It can make teachers feel more that the school principal cares about teachers' opinions in decisions regarding schools and classes.

- The school principal can increase his/her efforts to keep the discussions within the organization to a minimum. The higher the principals' communication with teachers and their knowledge of the problems, the earlier they will be able to act to prevent problems that may occur.

- Teachers can increase their use of technological innovations. Thus, students' interest in the course will increase.

- School principals and Ministry of National Education officials can initiate various studies to improve the technological infrastructure in schools.

- More parent meetings can be organized in order to increase parents' interest in education.

REFERENCES

[1] Abazaoğlu, İ., & Aztekin, S. (2015). Öğretmen Moral ve Motivasyonlarının Öğrencilerin Fen ve Matematik Başarılarına Etkisi. *"ICEFIC 2015 International Congress on Education for the Future: Issues and Challenges* (s. 16). Ankara: Pegem A. Yayıncılık.

[2] Açiler, Sezer. (2020). Nitel Araştırma Yöntemleri. İstanbul İşletme Enstitüsü. (İnternet Sitesi: https://www.iienstitu.com/blog/nitel-arastirma-yontemleri)

[3] Aydın, M. (2011). *Çağdaş Eğitim Denetimi*, Hatipoğlu Yayınevi.

[4] Avanoğlu, E. (2018). *Öğretmenlerin İletişim Becerileri ile Moralleri Arasındaki İlişkinin İncelenmesi* (Yayınlanmamış Yüksek Lisans Tezi). Kastamonu Üniversitesi, Kastamonu.

[5] Başıbüyük, K. (2012). *İlköğretim Okulu Öğretmenlerinin İşe Bağlılıkları İle Moral Durumları Arasındaki İlişki* (M.S. Thesis). Maltepe Universitesi.

[6] Eren, E. (2012). *Örgütsel Davranış ve Yönetim Psikolojisi*, İstanbul: Beta Yayıncılık.

[7] Ersoy, E. & Başer, N. (2010). *Probleme Dayalı Öğrenme Sürecinin Öğrenci Motivasyonuna Etkisi.* Turkish Studies International Periodical For the Languages, Literature and History of Turkish or Turkic Volume 5/4 Fall. p. 336-357. 2010. AnkaraTurkey.

[8] Tanrıöğen, A. (1995). *Öğretmen Moraline İlişkin Yapılan Araştırmalar,* Eğitim Yönetimi, 1, 1, 95-108.

[9] Tutum, C. (1979). *Personel Yönetimi*, Ankara: Doğan Basımevi.

[10] Yıldırım, A. & Şimşek, H. (2018). Sosyal Bilimlerde Nitel Araştırma Yöntemleri. Ankara: Seçkin Yayınevi

Scaling Smart: The Best Hosting Server Types for Multi-User Projects: Prof Dux as a use Case

Sarumi Usman Abidemi[1], Gresmarteneanos Tannous [2], Cliford Peter Mlimwa [3], Ibrahim Ame [4], Nafiseh Yousefi Kian[5], Sinem Alturjman, & Fadi Al-turjman[6]*

Artificial Intelligence Engineering Dept., Research Center for AI and IoT, AI and Robotics Institute, Near East University, Nicosia, Mersin 10, Turkey.

Correspondence: Sarumi Usman Abidemi, sarumiusman.abidemi@neu.edu.tr

ABSTRACT

The demand for scalable, efficient, and cost-effective hosting solutions is critical for multi-user applications due to existing issues that affect the efficient satisfaction and suitability implementation. This article evaluates different hosting server types—shared, virtual private servers (VPS), dedicated, and cloud hosting—analyzing their pros and cons in suitability for multi-user environments through comparative analysis from existing users projects. Our approach stated the best hosting solution considering scalability performance, cost efficiency and security as proposed solution to adaptive personalize education learning platform – Prof Dux as case study for scalable performance. More so, this analysis provide an insight to assist business and developer when making and informed decisions on hosting application for multiple users.

Keywords: *Hosting, server. Cloud. Dedicated server. Shared server. AWS, Google cloud, Prof Dux*

1. INTRODUCTION

A variety of real-time web approaches have been developed to address the issue of giving users changes as they happen on the server. These methods, which are predicated on the means of communication between the client and server, adhere to a number of ideas for providing such a service (Aziz, 2019). Multi-user applications, such as e-learning platforms, social media sites, and collaborative tools, require robust hosting solutions to ensure seamless functionality. One significant development that enables more adaptability and responsiveness is the rise of flexible and networked leadership structures.

By maximizing resource allocation and facilitating more effective decision-making, organizations that successfully use digital technology get a competitive advantage. However, managing the difficulties brought about by globalization is still a worry since firms need to combine regional adaptability with centralized management (Ma & Ye, 2015)

Selecting an appropriate hosting server impacts system reliability, security, and scalability This article explores different hosting options and their effectiveness for multi-user projects that attain more effective real-time client-server communication, but there are problems that limit their applicability and user satisfaction for an implementation.

2. LITERTATURE REVIEW

This section discussed about several existing research that provide insight into other edgeassisted mobile apps, considering the diverse array of use cases for mobile edge computing, dwelling into their pros and drawback. the author of this study examined shared, virtual private servers (VPS), dedicated, and cloud hosting for multiple users setup , a proof-of-concept was created , and its shown that, in the case of an overloaded edge server, it can achieve both a considerable decrease in AR latency and high object-recognition accuracy (Aziz, 2019).

Recently, discussed the advancement of containerization and serve less computing. Further shift hosting paradigms towards more flexible solution. Studies explore hosting server types and their application to various projects by explore cloud hosting's elasticity and cost-effectiveness in handling dynamic workloads (Aziz, 2019). Multi user always experience low traffic which make it unsuitable for the users , highlight hosting that’s offers affordability but lacks performance scalability (Vachhani et al., 2024). VPS hosting provides a middle ground between shared and dedicated hosting, offering resource allocation at a moderate cost (Almurayh, n.d.)

3. METHODOLOGY

In this chapter, a comparative analysis was conducted on different types of hosting server using key performance indicators (KPIs) such as latency, cost efficiency, uptime , security and scalability. The data’s are gathered through case studies of exiting multi0user platform and benchmarking reports from industry such as Google cloud. Microsoft Azure and AWS.

Case study: Uses single server to each user division (Dedicated server). (Gonzalez & Wang, 2017)

Pros:

- No concerns about server capacity or resource competition.
- Each school has full control over its own server.
- Dedicated resources often exhibit high performance.

Cons:

- High upfront costs for hardware and maintenance.
- Increased complexity in terms of management, updates, and security.
- Potential for inconsistent configurations.

Case study: Use a single server for multiple users division (Shared server). (Almurayh, n.d.)

Pros:

- Reduced hardware costs.
- Simplified management and updates.
- Potential for consistent configurations.

Cons:

- Risk of server overload or resource competition.
- Security concerns if one school's issues affect others.
- Potential for performance degradation due to resource sharing.

Case study: Use a middle ground server between dedicated server and shared server (Virtual private servers) (Lee & Kim, 2020)

Pros:

- Its cost effective for medium sized applications and also scalable
- VPS has better customization and greater control that share hosting

Due to its isolated resources , its more secure and offers better performance

Cons:

- Its resources are limited in comparison to dedicated server
- Required technical expertise for some level of server management

Case study: Use a Cloud hosting server (Miller, 2022).

Pros:

- It ensure high availability due to its redundant architecture
- Very flexible and scalable
- Cost efficiency such as Pay-as-you-go Cons:
- It requires knowledge of configuration on cloud space
- Cost is not fixed, as it depend on the services provider and resources

4. RESULT

This section entails about the outcome of this research its was suggested that Shared hosting is unsuitable due to resource limitations, while VPS offers a viable alternative for medium-scale applications, while dedicated servers remain relevant for high-security projects, and cloud hosting provides the best balance of scalability, performance, and cost efficiency for multi-user applications [18] [19].

How other companies handle similar situations:

Many web hosting companies and cloud service providers offer scalable solutions to handle the needs of multiple clients. Some common approaches include [20][21]:

Cloud Hosting: When resources are needed, cloud hosting enables website and application operators to add or delete them. This covers additional RAM, storage capacity, or auxiliary services like data storage or security. Cloud hosting offers affordability, flexibility, and dependability. Unlike dedicated or shared hosting on a single server, cloud hosting also offers reliable data backup and disaster recovery (*What Is Cloud Hosting? Benefits and Risks | Google Cloud*, n.d.) [22] [23].

Services like Google Cloud Platform as shown in figure 1 or AWS (Amazon Web Services) as shown in figure 2 provide scalable resources and managed services to handle high traffic and demands.

Figure 1: like Google Cloud Platform

Figure 2: AWS (Amazon Web Services)

Containerization and Orchestration: Companies like Kubernetes or Red Hat OpenShift use containerization and orchestration to manage and scale resources more efficiently.

1. **Containerization:** It involves combining the application code with the necessary packages and libraries needed at runtime so that the program can operate efficiently and dependably in any supported computing environment. Everything required to run an application is included in the

bundle or container, including the code, runtime, system tools, system libraries, settings, and more. Also known as a container image [24][25].

2. **Orchestration:** It all comes down to managing container lifecycles, particularly in expansive, dynamic environments. Numerous tasks can be controlled and automated with it.

Container deployment and provisioning : Container availability and redundancy for Increasing or decreasing the number of containers to distribute the application load uniformly throughout the host infrastructure, Transferring containers between hosts in the event that a host runs out of resources or passes away. Resource distribution among containers services operating in a container are exposed to the external environment. Service discovery load balancing between some containers orchestration platforms, like Docker Swarm or Kubernetes, offer a simple way to specify the configuration of your application in a YAML or JSON file, depending on the tool,

1. Multi-Tenancy: Some hosting companies implement multi-tenancy solutions, where multiple clients share a single infrastructure while maintaining isolation and security.

A single instance of a software program can serve numerous clients under a multi-tenancy architecture. Every client is referred to as a renter. Although they cannot alter the application's code, tenants may be allowed to change certain aspects of it, such as the user interface's color or the business rules.
A shared environment is used by several instances of an application in a multi-tenant architecture. Because each tenant is logically distinct yet physically integrated, this architecture can function. This implies that a single instance of the program will serve several tenants on a single server. A dedicated instance of configurations, data, user management, and other properties can be shared by a software program in a multi-tenant architecture in this manner (*What Is Multi-Tenancy (MultiTenant Architecture)?*, n.d.).

2. Multi-tenant SaaS Architecture: One application serves multiple schools with data separation (*What Is SaaS Architecture? 10 Best Practices In 2024*, n.d.).

Software as a Service, or SaaS, is a contemporary method of providing large, scalable enterprise software online. Scalability, availability, and utility computing for Internet services are offered via cloud computing platforms. The creation of SaaS involves numerous technical difficulties. One of these is multi-tenancy, which enables a single software instance to support numerous businesses by simultaneously configuring it to meet each one's specific needs. For SaaS architecture to reach

a higher maturity model, both configuration and some degree of customization are necessary (Aghera et al., 2012). https://ieeexplore.ieee.org/abstract/document/6200688

1. Content Delivery Network (CDN): To improve website speed globally. Reducing latency, or the communication lag brought on by a network's architecture, is the main goal of a content delivery network (CDN). Communication traffic between websites (servers) and their users (clients) must travel over great physical distances due to the internet's global and intricate structure. Additionally, the connection is two-way; the client sends requests to the server, and the server responds (*What Is a Content Delivery Network (CDN)*

By placing intermediary servers between the client and the website server, a CDN increases efficiency. Some of the client-server communications are controlled by these CDN servers. They enhance the user experience of your apps, lower bandwidth usage, and lessen web traffic to the web server (Peng, 2004).

Load Balancing: Distributing traffic to avoid overloading a single server. Load balancers, both cloud-based and software-based, aid in equitably allocating Internet traffic among the servers hosting the application. Global server load balancing (GSLB) is a technique used by some cloud load balancing providers to distribute Internet traffic loads among servers located all over the world (*Managed Cloud Hosting | 4X More Speed | 99.9% Uptime*, n.d.).

5. CONCLUSION

To choose the right hosting server for multi user application requires a crucial decision, in which some factors must be put into consideration for efficient performance, cost, security and scalability for Prof Dux personalize adaptive E-learning platform, due to increase in the number of users ranging from different departments and faculties from the university. This propose solution tend to explore different types of hosting server. Dedicated servers remain the preferred choice for enterprises that demand the highest security and performance levels, albeit at a higher cost. Shared hosting, while affordable, is not suitable for multi-user projects due to its limited resources and scalability constraints. Cloud hosting emerges as the most suitable option due to its flexibility, scalability, and cost-effectiveness, making it ideal for applications with fluctuating traffic and high availability requirements. VPS hosting provides a balanced approach for medium-sized applications that require more control than shared hosting but do not necessitate a dedicated server.

Ultimately, the choice of hosting server depends on the specific needs of the project, including budget, performance requirements, and security concerns for Prof Dux expansion project.

6. FUTURE STUDY

As technology evolves, future research should explore investigation into sustainable and energy- efficient hosting infrastructures will be essential as the demand for eco-friendly data centers grows. Comparative studies on hybrid cloud solutions and their potential to optimize performance and cost for multi-user applications should also be examined to provide a more comprehensive understanding of modern hosting strategies. Additionally, further investigation into sustainable and energy-efficient hosting infrastructures will be essential as the demand for eco-friendly data centers grows.

REFERENCES

[1] [1] Aghera, P., Chaudhary, S., & Kumar, V. (2012). An approach to build multi-tenant SaaS application with monitoring and SLA. *Proceedings - International Conference on Communication Systems and Network Technologies, CSNT 2012*, 658–661. https://doi.org/10.1109/CSNT.2012.146 [2] Almurayh, A. (n.d.). *Virtual Private Server*.

[2] Aziz, H. M. (2019). *REDUCING CLIENT-SERVER COMMUNICATION FOR EFFICIENT REAL-TIME WEB APPLICATIONS*.

[3] Chen, Y., Lin, X., & Zhou, L. (2019). "Elastic Cloud Hosting for Dynamic Workloads." *Journal of Cloud Computing, 7*(3), 112-125.

[4] Doe, J., & White, K. (2021). "Containerization vs Traditional Hosting: A Comparative Study." *Computer Science Review, 15*(1), 78-95.

[5] Gonzalez, R., & Wang, P. (2017). "Security and Cost in Dedicated Hosting." *IT Infrastructure Journal, 9*(4), 220-233.

[6] Lee, S., & Kim, H. (2020). "VPS Performance in Scalable Applications." *Journal of Web Hosting, 5*(2), 88-102.

[7] Ma, L., & Ye, M. (2015). The Role of Electronic Human Resource Management in Contemporary Human

[8] Resource Management. *Open Journal of Social Sciences*, *03*(04), 71–78. https://doi.org/10.4236/JSS.2015.34009

[9] *Managed cloud hosting | 4X more speed | 99.9% uptime*. (n.d.). Retrieved February 28, 2025, from https://www.hostinger.com/cloud-hosting?utm_campaign=Generic-Hosting%7CNT:SE%7CLO:Other-

[10] EU&utm_medium=ppc&gad_source=1&gclid=EAIaIQobChMI5aTz8InmiwMVcZeDBx37PhspEAAYAiAAEgIEifD_BwE

[11] Patel, R., Singh, M., & Verma, T. (2018). "Shared Hosting Limitations in Multi-User Systems." *International Journal of Computing, 4*(1), 32-47.

[12] Peng, G. (2004). *CDN: Content Distribution Network* *.

[13] Smith, A., & Jones, B. (2020). "VPS vs. Dedicated Hosting: Performance Trade-offs." *Computing Systems Journal, 12*(5), 99-120.

[14] Vachhani, M., Patel, Z., Garg, D., Patel, K., & Patel, M. (2024). Enhancing Cloud Computing Efficiency:

[15] Dynamic and Predictive Resource Allocation and Load Balancing Strategies. *Proceedings of 5th International Conference on IoT Based Control Networks and Intelligent Systems, ICICNIS 2024*, 16–20. https://doi.org/10.1109/ICICNIS64247.2024.10823380

[16] *What is a content delivery network (CDN)? | How do CDNs work? | Cloudflare*. (n.d.). Retrieved February 28, 2025, from https://www.cloudflare.com/learning/cdn/what-is-a-cdn/

[17] *What is Cloud Hosting? Benefits and Risks | Google Cloud*. (n.d.). Retrieved February 28, 2025, from https://cloud.google.com/learn/what-is-cloud-hosting

[18] *What is multi-tenancy (multi-tenant architecture)?* (n.d.). Retrieved March 3, 2025, from https://www.techtarget.com/whatis/definition/multi-tenancy

[19] *What Is SaaS Architecture? 10 Best Practices In 2024*. (n.d.). Retrieved February 28, 2025, from https://www.cloudzero.com/blog/saas-architecture/

[20] Kumar, R., Kumar, A., Gupta, M., & Chauhan, B. (2021, December). Quora based insincere content classification & detection for social media using machine learning. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 294-299). IEEE.

[21] Gupta, M., Kumar, R., Arora, A., & Kaur, J. (2022, December). Fuzzy logic-based Student Placement Evaluation and Analysis. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1503-1507). IEEE.

[22] Gupta, M., Kumar, R., Yadav, U., & Tuteja, D. (2022, September). Augmented reality based 3d business card implementing virtual buttons. In *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)* (pp. 1-6). IEEE.

[23] Kumar, R., Gupta, M., Bedi, K. S., Upadhyay, A., & Obaid, A. J. (2023, December). Earthquake Prediction Using Machine Learning. In *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 195-198). IEEE.

[24] Juneja, A., Kumar, R., & Gupta, M. (2022, December). Digitization of Traditional Markets using DART based Cross Platform Development. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 2272-2276). IEEE.

[25] Gupta, M., Ved, C., Khetarpaul, S., Dhingra, A., & Deswal, S. (2023). The emergence of blockchain technology in industrial revolution 5.0. *Privacy Preservation of Genomic and Medical Data*, 283-326.

A Survey on Secure Smart Homes in the Age of IoT- Enabled Smart Cities

Muhammad Furqan Zia[1], Maria Siddiqua[2], Fadi Al Turjman[3]

[1]*Department of Electrical and Computer Engineering, University of Quebec at Trois-Rivieres, QC, Canada*
[2]*Department of Artificial Intelligence and Data Science, The National University of Computer and Emerging, Sciences (FAST-NUCES), Karachi, Pakistan*
[3]*Department of Information Systems, AI and Robotics Institute, Near East University, Nicosia, Türkiye*

Muhammad.Furqan.Zia@uqtr.ca, Maria.Siddiqua@nu.edu.pk, Fadi.alturjman@neu.edu.tr

ABSTRACT

The rapid growth of urban areas and advancements in information technology have paved the way for the development of smart cities and homes, leveraging the Internet of Things (IoT). Smart cities and homes represent the future of urban living, offering enhanced efficiency, convenience, and sustainability. This survey paper provides a comprehensive overview of the progress made in the domain of smart homes, focusing on the integration of IoT technologies. It explores the architectures, applications, devices, and communication technologies that have been implemented to achieve desired outcomes in smart home environments. Additionally, the paper highlights the key challenges researchers are addressing, particularly in the realm of security, to ensure the safe and reliable operation of smart homes within smart cities. By examining the current state of the art, this paper aims to provide insights into the future direction of secure smart homes and their role in the broader ecosystem of smart cities.

Keywords: *Smart city, IoT security, Home Automation, Communication technologies, IoT challenges, Secure Smart homes.*

1. INTRODUCTION

The proportion of the global population living in cities has surpassed 50% and is projected to reach 70% by 2050 [1]. This rapid urbanization has intensified the demand for efficient resource management, improved governance, and enhanced quality of life. To address these challenges, the concept of smart cities has emerged, leveraging advancements in information and communication technologies (ICT). A smart city is a self-sustaining ecosystem that integrates advanced technologies such as IoT, sensors, base stations, and communication protocols, all managed through sophisticated databases and algorithms [2]. At the core of a smart city lies the concept of smart homes, which are residential units equipped with advanced technologies to automate and optimize daily operations, ensuring energy efficiency, security, and convenience. Smart homes are revolutionizing traditional living spaces by incorporating IoT-enabled devices such as cameras, motion sensors, fire alarms, and smart appliances. These devices collect and analyze data to automate tasks, reducing the need for human intervention. For instance, a smart home can adjust lighting, temperature, and security systems based on real-time data, ensuring optimal functionality and energy savings [3]. The integration of smart homes into smart cities has led to the development of various applications, including smart grids, smart meters, water management systems, healthcare monitoring, and surveillance systems [4]. These applications aim to enhance resource utilization, improve governance, and provide better services to urban residents.

Despite the significant progress in smart home technologies, several challenges remain, particularly in the areas of security, privacy, and interoperability. Researchers and industry experts are actively working to address these issues to ensure the safe and efficient deployment of smart homes in smart cities. This survey focuses on the automation of smart homes within the broader context of smart cities. It provides a comprehensive analysis of the architectures, devices, communication technologies, and techniques used in smart home systems. Additionally, the paper highlights the challenges and open research issues in this domain, offering insights into future directions for secure and efficient smart home deployment.

The paper is organized into several sections to provide a structured overview of the topic. Section II discusses the background, objectives, and constraints of smart homes in smart cities. Section III explores existing and emerging applications of smart home technologies. The architecture and fundamental components of smart homes, along with trustworthy computing models, are detailed in Sections IV and V. Section VI categorizes the devices used in smart homes, while Section VII and VIII explain secure deployment strategies and wireless communication protocols, respectively. Section IX addresses critical challenges such as security and privacy, along with potential countermeasures. Section X provides insights into the deployment of smart homes, and Section XI identifies open research issues to guide future studies. Finally, Section XII concludes the paper by summarizing the key findings and their implications for the future of smart homes in smart cities.

To assist readers, a list of abbreviations and their definitions is provided in Table I. This paper aims to serve as a valuable resource for researchers and practitioners seeking a unified understanding of secure smart homes in the context of smart cities. By covering a wide range of aspects, this survey paper contributes to the ongoing efforts to create smarter, safer, and more sustainable urban living environments.

Table 1. *Table of Abbreviations*

Term	Abbreviation
IoT	Internet of things
LAN	Local Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
RFID	Radio-frequency identification
WPAN	Wireless Personal Area Network
DDoS	Distributed Denial of Service
PDoS	Permanent Denial of Service
Wi-Fi	Wireless Fidelity
GSM	Global System for Mobile Communications
BLE	Bluetooth Low Energy
SIG	Special Interest Group
LTE	Long-Term Evolution
UMTS	Universal Mobile Telecommunications System
DNS	Domain Name System

2. BACKGROUND

As urban populations continue to grow, cities face significant challenges in resource management, infrastructure sustainability, and disaster resilience. Addressing these challenges is crucial to enhancing the quality of life for citizens. One of the most promising solutions is the development of smart cities, which leverage advanced technologies to create more efficient, sustainable, and adaptable urban environments.

Smart cities integrate wireless technologies to optimize resource utilization and improve disaster preparedness. Wireless communication facilitates seamless connectivity among various urban components, such as smart grids, intelligent transportation systems, automated surveillance, and environmental monitoring. These interconnected systems enhance efficiency, reduce costs, and provide better solutions for managing urban infrastructure.

A smart city, along with smart homes, relies on essential components such as smartphones, sensors, and networks to function effectively in a wireless and mobile environment. Sensors play a crucial role in monitoring and supporting infrastructure, including smart grids, home automation, surveillance systems, vehicular navigation, and even earthquake detection in buildings. The deployment of wireless networks enables real-time communication among these devices, ensuring better decision-making and automated responses to various urban challenges.

Wireless networks use radio waves as the primary communication medium, offering advantages such as flexibility, cost- effectiveness, and ease of deployment. Several types of networks are utilized in smart city applications, each with unique advantages. These include Local Area Networks (LAN), Wide Area Networks (WAN), Metropolitan Area Networks (MAN), WiMAX, Wi-Fi, and Zigbee. Each of these technologies plays a critical role in enabling smart city functionalities and ensuring seamless communication across various components of the ecosystem.

Objectives: The primary objective of research in smart cities and smart homes is to develop and deploy cost-efficient, high- performance infrastructure. Key research studies have explored various aspects of smart home automation and security:

In [7], researchers focused on building cost-effective smart homes with enhanced security features.

In [8], different automation techniques were examined, such as control via web browsers, cloud servers, GSM, and Bluetooth.

In [9], security challenges in smart homes were analyzed, including authentication, integration, and standardization issues.

In [10], a mobile application was proposed to control multiple home appliances remotely using IoT, providing flexibility and improved security.

In [11], various home automation methodologies were discussed, highlighting innovations in automation frameworks. The proposed smart home and city frameworks aim to offer greater automation flexibility, improved security, and enhanced management solutions for water conservation and child safety.

Constraints: Despite the advancements in smart city and home automation technologies, several constraints hinder widespread implementation. Key challenges identified in literature include:

Cost Efficiency: Studies such as [7] emphasize the high cost of smart home deployment, including equipment, installation, wiring, and development expenses. Researchers explore methods to reduce these costs while maintaining performance.

- **Internet Connectivity**: In [8], challenges in maintaining a stable internet connection, particularly in rural areas, are highlighted. Continuous internet access is necessary for cloudbased smart home solutions, posing a barrier in low- connectivity regions.
- **Security Concerns**: Research in [9] discusses issues related to controlling multiple devices simultaneously, ensuring data security, and addressing integration challenges within smart homes.
- **Communication Efficiency**: In [11], various communication techniques were evaluated based on cost, efficiency, and data transmission rates.
- **System Vulnerabilities**: Security concerns related to smart home automation systems were elaborated in [12], emphasizing the potential threats that could compromise the functionality of connected devices.

The following table summarizes key constraints associated with smart home implementations across different research studies.

3. APPLICATIONS

In recent years, engineers and researchers have made significant strides in developing innovative applications for smart homes. These applications leverage a variety of sensors—such as motion, light, fire, and environmental sensors—to detect activities and gather data. The collected information is then processed to trigger appropriate actions, enhancing convenience, security, and energy efficiency. Below is an in-depth exploration of the key applications currently being utilized in smart homes:

3.1. Smart Lighting

Smart lighting systems are revolutionizing the way we interact with lighting in our homes. These systems require smart bulbs, motion sensors, light sensors, and a wireless connection to enable control via mobile applications. Users can manage their lighting remotely through internet or Bluetooth connections. Additionally, motion and light sensors automate lighting control by adjusting brightness or turning lights on/off based on occupancy and ambient light levels. For instance, lights can dim during the day when natural light is sufficient or turn on automatically when someone enters a room. Research by [13] provides a detailed analysis of lighting control systems in smart homes, highlighting their energy-saving potential and user convenience.

3.2. Smart Garage

The smart garage is a cornerstone of modern home automation, with its primary functionality being the automated garage door opener. These systems often employ rolling-code technology, such as the KeeLoq lightweight block cipher, to generate secure, cryptographically encoded signals. When a user syncs their remote control with the garage door opener, both devices generate matching codes in the same sequence, ensuring secure access. Advanced systems also integrate with mobile apps, allowing users to monitor and control their garage doors remotely. In [14], the author delves into the security measures and operational functionalities of smart garage systems, emphasizing their role in enhancing home security.

Smart Meters

Smart meters are fundamental to energy management in smart homes. These devices provide real-time monitoring and control over energy-consuming units within the home. A typical smart meter consists of three main sections:

• **Base Station**: Includes components like IoT gateways, appliance trackers, and data repositories.
• **Appliance Controller**: Equipped with sensors and relay modules to manage connected devices.
• **User Interface**: Allows homeowners to monitor energy consumption patterns and optimize usage.

By providing detailed insights into energy usage, smart meters empower users to reduce waste and lower utility bills. Reference [15] offers a comprehensive explanation of smart meter functionality and their role in promoting sustainable energy practices.

Smart Kitchen

The kitchen is a focal point of smart home automation, with a wide range of intelligent appliances designed to simplify daily tasks. For example:

• **Smart Refrigerators**: Devices like LG's Smart ThinQ can scan grocery receipts, track inventory, and send alerts when items are nearing expiration. They can also suggest recipes based on available ingredients.

• **Energy Monitoring**: By automating kitchen appliances and accessing them via smartphones, users can monitor energy consumption and reduce waste.

These innovations not only enhance convenience but also contribute to energy efficiency and sustainability. Reference [16] explores the integration of smart kitchen appliances and their impact on modern living.

HVAC Regulation

Heating, ventilation, and air conditioning (HVAC) systems account for nearly 50% of a home's annual energy costs. Smart HVAC systems optimize energy usage by adjusting temperatures based on occupancy and user schedules. For instance, the system can lower heating or cooling when a room is unoccupied and restore comfort levels before occupants return. Advanced systems also integrate weather forecasts to further enhance efficiency. Reference [16] discusses the benefits of automated HVAC systems in reducing energy consumption and improving home comfort.

Lawn Irrigation Systems

Maintaining a lush and healthy lawn can be challenging, especially with unpredictable weather conditions. Traditional sprinkler systems often waste significant amounts of water due to inefficiencies. Smart irrigation systems, such as Skydrop, address this issue by leveraging realtime weather data to optimize watering schedules. For example, if rainfall provides sufficient moisture, the system will automatically disable scheduled watering, conserving water and reducing costs. Reference [16] highlights the environmental and economic benefits of smart lawn irrigation systems.

Smart Security

Home security is a top priority for homeowners, and smart security systems offer advanced solutions to safeguard properties. These systems typically include:

• **CCTV Cameras**: Provide real-time surveillance and recording.
• **Motion Sensors**: Detect unauthorized movement and trigger alarms.
• **Biometric Devices**: Enable secure access through fingerprint or facial recognition.
• **Automated Alerts**: Notify homeowners and authorities in case of a security breach.

By integrating these components, smart security systems provide robust protection and peace of mind. Reference [16] explores the latest advancements in home security technologies and their effectiveness in deterring intruders.

Emerging Applications

Beyond the applications mentioned above, smart home technology continues to evolve, introducing new possibilities such as:

• **Smart Health Monitoring**: Integration of wearable devices and health sensors to track residents' well-being.
• **Voice-Activated Assistants**: Systems like Amazon Alexa and Google Home enable handsfree control of various smart devices.
• **Energy Storage Systems**: Integration with solar panels and home batteries to optimize energy usage and reduce reliance on the grid. In the forthcomings ection, we will delve into the architecture and core components of smart homes, providing a deeper understanding of how these systems are designed and integrated.

3. ARCHITECTURE AND MAIN COMPONENTS

Smart home systems comprise several essential components, including sensors, actuators, wireless signal control devices, appliances, and monitoring systems. Sensors play a crucial role in detecting various activities such as light intensity, motion, and temperature. Actuators are responsible for executing mechanical movements and controlling various home automation mechanisms. These actuators require a power source and a controlled signal to function efficiently. Wireless signal control devices, such as modems, facilitate seamless communication between different components. Additionally, smart appliances like refrigerators, air conditioners, and washing machines enhance convenience, while surveillance devices such as cameras and monitoring screens improve security.

Various architectural models have been proposed for smart home implementation within smart cities. Among these, researchers widely recommend a three-layered architecture for smart home automation [17]. This model comprises:

1. **Sensing Layer** 2. **Network Layer** 3. **Application Layer**

Each of these layers plays a critical role in the overall functionality of a smart home system.

Sensing Layer

The sensing layer is responsible for collecting data from different home appliances and environmental conditions within a household. Sensors embedded in appliances, doors, and other household items gather data on temperature, light, motion, and other factors. These sensors transmit data to microprocessors such as the SAMSUNG S3C2440A, which process and forward the information. Wireless modules like ZigBee [9] enable communication between the sensing layer and the next stage in the architecture.

Network Layer

The network layer serves as an intermediary, gathering data from the sensing layer via wireless communication technologies such as Wi-Fi and ZigBee. It efficiently transfers the collected data to the application layer while employing various network protocols to ensure optimal data transmission. This layer acts as a bridge, facilitating seamless data exchange between lower and upper layers.

Application Layer

The application layer, the topmost layer in this architecture, receives data from the network layer and utilizes it for various automation purposes. Typically, applications installed on smartphones allow users to control home appliances remotely. Notable smart home applications include Nest and Samsung SmartThings [18]. Users can leverage these applications to manage home settings wirelessly, enhancing convenience and energy efficiency.

4. TRUSTWORTHY COMPUTING MODELS

Several trustworthy computing models have been developed for smart homes, each offering unique advantages and features. Different modeling techniques include feature modeling and variability modeling. In [37], the author introduced an object- based IoT management model, while in [38], a ZigBee-based smart home system was analyzed. Based on the literature, many researchers favor feature modeling due to its robust support for variability reasoning and system functionality enhancement. In [39], the author explored feature modeling in the context of smart homes, illustrating how features are organized in a hierarchical tree structure with variability relationships such as optional, mandatory, single-choice, and multiple-choice options. The figure below represents a smart home feature model, incorporating automated illumination, multimedia systems, garage management, and security functionalities. The blue boxes highlight active features, whereas black boxes indicate potential future variations.

A. Techniques In Home Automation

Several techniques have been explored in the literature to enhance smart home automation, improving the efficiency and connectivity of home devices. These techniques can be broadly categorized into two main approaches:

1. **Voice Recognition-Based Home Automation**
2. **IoT-Based Home Automation** [19].

Voice Recognition-Based Home Automation:

A voice recognition-based home automation system was proposed and implemented by researchers [20]. The hardware setup includes an Arduino UNO microcontroller and a smartphone. Wireless communication between the Arduino and the smartphone is established using Bluetooth. Smartphones utilize built-in voice recognition commands, enabling users to control home appliances via voice input [11]. Furthermore, Android devices use Google Assistant, while iOS devices employ Siri for voice-controlled automation.

IoT-Based Home Automation:

A study [21] introduced a home control and monitoring system based on IoT technology. The system was designed and implemented using an embedded micro-web server, controlling devices, and a smart home software application. The proposed architecture consists of three key components:

1. **Home Environment:** Contains hardware interface modules and a home gateway to manage smart devices.
2. **Home Gateway:** Acts as a bridge between the home environment and external networks.
3. **Remote Environment:** Enables authorized users to monitor and control home appliances remotely via smartphones using Wi-Fi, 3G, or 4G networks.

Table3. *Comparison between Home Automation control Techniques*

Technology	Cost	Efficiency	Flexibility	Response
Voice Recognition	Moderate	Moderate	High	Moderate
IoT Based	High	High	High	High

5. DEVICES USED IN SMART HOMES

A wide range of devices are utilized in home automation to enhance convenience, security, and overall quality of life. These devices can be categorized as follows:

Sensing Devices

Smart homes incorporate various sensors designed to monitor and respond to environmental changes. These include:

- **Fire Sensors:** Detect smoke or fire and activate water sprinklers for fire suppression.
- **Moisture Sensors:** Identify moisture levels in walls, helping to prevent water damage and mold growth.
- **Motion Detectors:** Detect movement within the home and can trigger lighting or security alerts.
- **Light Sensors:** Measure ambient light levels and automatically turn lights on or off as needed.
- **Water Sensors:** Monitor water levels in tanks and help prevent overflow or shortages.
- **Pressure Sensors:** Detect pressure variations inside and outside the home, providing valuable data for home automation systems.
- **Gas Sensors:** Identify the presence of harmful gases, such as carbon monoxide or natural gas leaks, and trigger alerts for safety.
- **Other Sensors:** These include chemical sensors for detecting hazardous substances and thermostat sensors for climate control.

Appliances

Smart home automation extends to various household appliances, improving efficiency and convenience across different areas of the home:

- **Kitchen Appliances:** Refrigerators, kettles, juicers, microwaves, blenders, and cookers.
- **Washroom Appliances:** Washing machines, hand dryers, and toilet roll dispensers.
- **Living Room Appliances:** Air conditioners, fans, lights, and heaters.

Entertainment Devices

Smart homes integrate entertainment systems for leisure and recreation, including:

- **Home Theater Systems:** Smart TVs, DVD players, and high-quality speakers.
- **Gaming Devices:** Computers, monitors, gaming consoles such as Xbox and PlayStation.
- **Music Devices:** Smart speakers, sound systems, and microphones for immersive audio experiences.

Security Devices

Security is a fundamental aspect of smart homes, with various devices ensuring the safety of occupants:

- **CCTV Cameras:** Provide real-time surveillance and remote monitoring.
- **Alarms:** Trigger alerts in case of unauthorized access or emergencies.
- **Monitoring Screens:** Display live feeds from security cameras for enhanced surveillance.

By integrating these devices, smart homes offer a seamless, automated, and secure living environment, improving both comfort and safety.

Table 4. *Categories of devices in Home Automation*

Categories	Devices
SensingDevices	Fire,Moisture,Motion,Light, Water
Appliances	**Kitchen:**(Refrigerators, Kettles, Juicers, Microwave). **Washroom:** (Washing Machines, Hand Dryers, Toilet Roll Dispensers). **LivingRoom:**(AirConditioners, Fans,Lights,Heaters).
Entertainment Devices	**HomeTheaterDevices:**(TVs,DVD Box, Speakers). **Gaming Devices:** (Computers, Monitors, Xbox, PlayStation). **Music devices:** (Speakers, Microphones).
SecurityDevices	CCTV Cameras, Alarms and monitoringscreens

SECURE DEPLOYMENT OF SMART DEVICES

Ensuring the secure deployment of smart home devices is a major concern today. With the increasing number of security threats, it is essential to implement proper security measures when deploying these devices. Several techniques and parameters should be considered to enhance the security of smart home systems.

Device Reviews and Research

Before purchasing a smart home device, users should conduct thorough research and read reviews to assess its security and performance. Reviews can provide insights into whether a device has been previously targeted by hackers and how well it withstands cyber threats. A wellreviewed device with a strong security track record is less likely to be vulnerable to attacks.

Secure Connection Applications

It is crucial to verify the application that connects smart home devices. Users should check:

- The developer or company behind the application.
- The app's security rating and reviews.
- Whether the application receives regular updates to enhance security.

A well-maintained application with frequent updates is more likely to incorporate the latest security features, reducing the risk of vulnerabilities.

Password Protection

Most modern smart home devices support password protection. However, users should ensure that the device allows them to change the default password. Some manufacturers restrict password modifications, which increases security risks by making devices more vulnerable to attacks. Always opt for devices that allow customizable, strong passwords.

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) provides an additional layer of security by requiring two types of credentials for authentication. Typically, one factor is a physical validation token (e.g., a smart card or biometric scan), while the other is a logical code or password. Enabling 2FA significantly reduces the risk of unauthorized access.

Device Preparation and Authentication

Before integration into a smart home system, devices must undergo a secure setup process. This includes:

- Scanning the QR code on the device or selecting the correct product title from the app.
- The app retrieving a product_uuid and sending it to the cloud.
- The app broadcasting a PT_SCAN message containing the product_uuid and the application's EC public key.
- The application prompting the user to input Wi-Fi credentials and initiating Wi-Fi provisioning.

Secure Wi-Fi Provisioning

During the Wi-Fi setup of a headless IoT device, several common methods are used, such as Access Point Mode, Wi-Fi Direct, and TI's SmartConfig. JoyLink, for instance, follows a process where:

- The app encrypts the SSID and password into a series of IP addresses.
- The app transmits each IP address with a null character while simultaneously broadcasting the PT_SCAN message.
- The smart device detects the traffic pattern, extracts the Wi-Fi credentials, and connects to the network.
- The device then sends a PT_SCAN response to the app, which includes its MAC address and device key (EC public key).

Device Initialization

Once the app retrieves the MAC address, it sends a request to the cloud containing the MAC address, product_uuid, and user account details. The cloud verifies the ownership and responds with a message containing:

- feed_id and access_key
- A locally generated encryption key (local_key)

The app then encrypts the feed_id and access_key before sending them to the device using a PT_WRITEACCESSKEY message. The device stores these credentials and sends a PT_AUTH request to the cloud to authenticate itself. The cloud responds by generating a session_key, encrypting it with the access_key, and sending it back in a PT_AUTH response. This ensures secure remote communication.

Communication Security

For smart home deployment, secure communication protocols are essential to protect data transmission. Various security techniques, such as Key Management Systems (KMS), ensure authentication and encryption of data exchanges. Implementing these protocols minimizes the risk of cyber threats and unauthorized access.

SECURE COMMUNICATION PROTOCOLS

Various wireless communication technologies are used in home automation to ensure seamless connectivity, efficient data transfer, and reliable performance. Each technology has distinct features, such as data rate, range, and power consumption. Below is an overview of the most commonly used wireless communication technologies in smart home applications.

Wi-Fi

Wi-Fi is the most widely used wireless communication technology in home automation. Based on the IEEE 802.11 standard, it operates on 2.4 GHz, 3.5 GHz, and 5 GHz frequency bands and supports data rates of up to 300 Mbps. Wi-Fi offers high-speed and secure communication with a range of up to 100 meters [24]. Further advancements, such as small cell technology, can enhance Wi-Fi networks by improving spectrum efficiency and communication reliability [25].

LTE (Long-Term Evolution)

LTE, originally developed for high-speed data transfer between mobile devices, is based on GSM/UMTS standards [26]. The enhanced version, LTE-A (LTE-Advanced), supports higher bandwidths of up to 100 MHz, offering improved coverage, higher throughput, and lower latency [25]. **ZigBee**

ZigBee is a low-power, wireless personal area network (WPAN) technology based on IEEE 802.15.4. It is widely used in home automation due to its low data rate (up to 250 kbps) and long battery life (up to 10 years). ZigBee operates on multiple frequency bands, primarily 2.4 GHz, and has a typical transmission range of up to 100 meters, depending on power output and environmental factors.

Z-Wave

Z-Wave is a low-power, cost-effective wireless communication technology designed for remote control applications. It supports data rates of up to 40 kbps and has a coverage range of up to 30 meters. Operating on the 2.4 GHz frequency band, Z-Wave is commonly used in smart home security and automation.

Bluetooth & Bluetooth Low Energy (BLE)

Bluetooth is based on IEEE 802.15.1 and is widely used for short-range wireless communication. It operates on 2.4 GHz, supports data rates of up to 21 kbps, and has an operating range of up to 100 meters. Bluetooth is preferred for home automation due to its low power consumption, making it suitable for short-distance communication [27]. Bluetooth Low Energy (BLE) is a specialized version designed for low-power monitoring applications. Compared to classic Bluetooth, BLE consumes significantly less power and operates on the 2.4 GHz band, making it ideal for IoT applications [25].

EnOcean

EnOcean is an energy-harvesting wireless technology, meaning it generates power from natural sources such as ambient light. It is a cost-efficient solution for battery-less equipment and has extremely low maintenance costs. EnOcean operates on 902 MHz and 315 MHz, with a data rate of up to 125 kbps [24].

Wave2M

Wave2M is designed for ultra-low-power long-range transmission of small amounts of data. It can cover distances of up to 1000 meters, supports data rates of up to 100 kbps, and operates on the 2.4 GHz frequency band.

RFID (Radio-Frequency Identification)

RFID is a bi-directional radio frequency identification system that consists of tags and readers. It can be integrated with handheld computing devices or personal computers and can coexist with technologies such as ZigBee and Wi-Fi. RFID's detection range varies from 10 cm to 200 meters, supporting data rates of up to 4 Mbps and operating across a wide frequency spectrum of 120 kHz to 10 GHz.

ONE-NET

ONE-NET is an open-source standard for low-cost, low-power wireless networks. It is designed for applications such as home automation, security monitoring, device control, and sensor networks. ONE-NET supports a coverage area of up to 100 meters with data rates of up to 38.4 kbps, operating at 915 MHz.

Table5. *Comparison of wirelessTechnologies*

Technology	Cost	Power	Speed	Operating Frequency	Operating Range upto
WIFI	High	High	300 Mbps	2.4GHz	100
ZigBee	Low	Low	250Kbps	2.4GHz	100
Z-Wave	Low	Low	30Kbps	2.4GHz	30
Bluetooth	Low	Low	21Kbps	2.4GHz	100

IEEE 802.15.3a	High	High	20Mbps–1.3Gbps	3.1-10 GHz	10
EnOcean	Low	Moderate	125Kbps	315&902 MHz	30
Wave2M	Low	High	100Kbps	2.4GHz	1000
RFID	Low	Low	4Mbps	120KHz – 10GHz	10cm–200m
ONE-NET	Low	Low	38.4Kbps	915 MHz	100
LTE	High	High	50-100 Mbps	450-2600 MHz	Mobile

6. PROBLEMS AND CHALLENGES

Interoperability:

Interoperability refers to the ability of systems, applications, and services to work together seamlessly and predictably. It is a critical concern in smart home ecosystems, as consumers demand devices that are easy to connect and use. However, smart home devices often come from various vendors with different network interfaces, making interoperability essential for achieving joint task execution. While many devices now operate on widely adopted protocols like Wi-Fi and Zigbee, which facilitate interoperability across a broad range of devices, challenges remain. Although industry standards have been established, there are still areas requiring improvement. For instance, in [28], the author highlights the ongoing issues related to interoperability and connectivity in smart home systems.

Self-Management:

Intelligent systems in smart homes must be capable of self-monitoring and notifying users of potential issues before they escalate into critical situations. A key requirement for sensor nodes is the ability to adapt to environmental changes autonomously, without human intervention. These systems should also collaborate independently with other devices to ensure seamless operation. In [29], the author provides a detailed explanation of the self-management challenges faced by smart home systems, emphasizing the need for autonomy and adaptability.

Maintainability:

Maintainability is a crucial aspect of any smart home network, reflecting its reliability and durability over time. Networks must handle various changes, such as failing nodes, depleted batteries, and the introduction of new tasks. To address these challenges, the system should continuously monitor its performance and adjust operational parameters as needed. For example, it may need to prioritize energy efficiency by reducing data quality when resources are limited, as discussed in [29].

Bandwidth:

Bandwidth management is a significant challenge in IoT connectivity, especially as the number of connected devices continues to grow, generating massive amounts of data. Applications like video streaming, which demand high bandwidth, exacerbate this issue. To ensure smooth operation, smart home systems must be capable of transferring data efficiently, without delays or loss. This requires robust network design and optimization, as highlighted in [29].

Power Consumption:

Power consumption is a critical concern for IoT devices in smart homes. These devices constantly send and receive signals, and their CPUs process data, leading to significant energy use. An efficient IoT network must minimize energy consumption while maintaining high performance. However, there is a trade-off between power usage and data transmission: systems that send and receive more data will inherently consume more power. Striking the right balance is essential, as noted in [29].

Integration:

As the smart home industry grows, numerous companies are producing a wide variety of smart devices for homes and cities. While this provides consumers with a wealth of options, it also introduces integration challenges. Devices from different brands often operate on different frequencies or protocols, leading to compatibility issues and increased complexity. Addressing these integration problems is vital for creating a cohesive and user-friendly smart home ecosystem.

Data Storage:

The rapid growth of IoT applications has led to an exponential increase in data collection. Storing this vast amount of data requires significant storage capacity, which can drive up costs. Efficient data management strategies, such as cloud storage and edge computing, are essential to mitigate these challenges and ensure scalability.

High Cost of Ownership:

The adoption of smart home technology often involves significant upfront costs. Consumers need to purchase a variety of devices, including sensors, relays, smart appliances, and embedded systems. While these devices offer advanced functionality, their high cost can be a barrier to widespread adoption. The industry continues to face challenges in producing and installing smart equipment at affordable prices, making cost reduction a key area for innovation. By addressing these challenges—interoperability, self-management, maintainability, bandwidth, power consumption, integration, data storage, and cost—smart home systems can become more efficient, reliable, and accessible to a broader audience.

SECURITYAND PRIVACY REQUIREMENTS FOR SMART HOME SERVICES

Secure smart homes are a critical necessity in today's world. While these homes offer a variety of features, security remains the foremost concern for residents. To safeguard these homes, there are several essential requirements for security services. Numerous studies have explored the various security needs of smart homes. In [40], the author identifies some fundamental security and privacy requirements, including Data Confidentiality, Data Integrity, and Device-to-Device Authentication, among others. Additionally, security and privacy can be divided into several core categories such as confidentiality, integrity, and availability. By addressing and fulfilling these requirements, we can achieve a moderate level of security for smart homes. The following table outlines some of the key security requirements.

Table6: *Security and Privacy requirements for Smart Home*

Category	Security Requirement
User and Device Authentication	In a smart home, numerous devices are interconnected and rely on the internet for software updates, security patches, and data exchange. Only authorized users should be allowed to perform these functions. A robust authentication mechanism or key management technique is necessary to prevent unauthorized devices and users from gaining access. Withou such techniques, it is impossible to protect the smart home from adversaries [41][42].
Network Monitoring	In a smart home, various entities such as home appliances, Energy Storage Systems (ESS), and Renewable Energy Sources (RES) are connected to the network. Adversaries can target the smart home network via Denial of Service (DoS) attacks and other network-based threats. To defend against such attacks, it is essential to install monitoring and intrusion detection tools. Without these tools, it is not possible to secure the network from these types of threats.
Integrity	Integrity ensures that information cannot be altered by unauthorized users during any process, whether it's message requests, storage or transmission. Data must remain unaltered and intact at all stages. In other words, integrity guarantees that information is transmitted accurately and consistently. Adversaries often compromise integrity through malicious software attacks [44]. Message Authentication Codes (MAC) are commonly used to verify integrity.
Availability	Availability guarantees that network services and resources remain accessible at all times while being protected from malicious attacks. In the context of smart homes, malicious threats and DoS attacks can disrupt or expose network services and resources. Disaster recovery solutions are essential for ensuring the continued availability of services within the smart home network [43].
Confidentiality	Confidentiality ensures that users' private information remains secure and is only accessible by authorized individuals Cryptography and effective key managemen strategies are employed to maintain confidentiality and protect user data from unauthorized access [46].

t

,

Security Challenges:

Authentication: Authentication is the process of verifying the identity of communicating parties or users, ensuring that they are who they claim to be and that data is sent to the correct recipient. It is a fundamental aspect of security. Servers containing sensitive user information should grant access only to authenticated users. Solutions to combat these attacks include the use of strong passwords and the generation of random captchas [30].

Man-in-the-Middle Attacks: This occurs when an attacker intercepts or manipulates communication between two systems. For example, an attacker could fake temperature data from a sensor and send it to a server or cloud. To prevent such attacks, employing strong cryptographic methods, secure authentication, and data integrity checks are essential.

Data and Identity Theft: Data generated by insecure or poorly protected devices, such as wearables and home appliances, can be exploited by cybercriminals. Personal information can be stolen for fraudulent transactions and identity theft. Preventive measures include strengthening passwords, limiting the sharing of personal information, and protecting mobile devices with strong passwords [31].

Masquerading: In masquerading attacks, an entity masks its identity and impersonates another system or device using false identities, such as public keys. This technique is often used in conjunction with other attack methods. Prevention can be achieved by implementing a multistep approval process and identity verification.

Eavesdropping: Eavesdropping is a passive attack where an unauthorized third party intercepts ongoing communication without the consent of the communicating parties. This can include phone calls, instant messages, or other forms of internet-based communication. Encryption is the most effective solution to prevent this type of attack.

Device Hijacking: In device hijacking, a hacker takes control of a smart device and uses it for malicious purposes. These attacks are difficult to detect because the basic functionality of the device remains unchanged, making it hard for users to notice. A single compromised device can infect other devices within the home. For instance, an attacker who compromises a thermostat may gain access to locks or other appliances, even changing PINs to restrict access for authorized users. To prevent device hijacking, it is crucial to strengthen passwords and regularly update device software [32].

Distributed Denial of Service (DDoS): A denial of service (DoS) attack occurs when an attacker renders a device or network resource temporarily unavailable to authenticated users. In DDoS attacks, multiple sources are involved, making it difficult to stop the attack by blocking a single source. For example, a compromised smart sensor could infect devices running the same software. To prevent these attacks, it is essential to deploy anti-DDoS hardware and software modules and protect DNS servers.

Permanent Denial of Service (PDoS): In PDoS, the damage caused by the attack is so severe that it permanently damages the device, necessitating its replacement or reinstallation. For example, BrickerBot exploits hard-coded passwords in IoT devices to cause permanent denial of service. Solutions to mitigate these risks include protecting DNS servers and strengthening firewall security.

False Information: Attackers may transmit erroneous or manipulated information within the network, which can negatively impact the behavior of other devices or systems. This can be either intentional or unintentional, leading to misinformed actions or decisions.

Security Countermeasures:

To secure connected smart home devices, a comprehensive IoT security solution (device-tocloud) should be implemented. This solution should not disrupt a service provider's or OEM's profitability or time-to-market. A comprehensive security solution should incorporate the following capabilities [47] [48]:

Secure Boot: Secure boot uses cryptographic code-signing techniques to ensure that devices only run code generated by the device's OEM or another trusted party. With secure boot, hackers cannot replace the device's firmware with malicious code, helping to maintain the device's integrity.

Mutual Authentication: When a smart home device connects to the network, it should undergo authentication before transmitting or receiving data. This ensures that the data originates from a legitimate device and source. Various cryptographic algorithms, such as Secure Hash Algorithm (SHA) and Digital Signature Algorithm (DSA), can be used for two-way authentication.

Secure Communication (Encryption): Encrypting data in transit between devices and their service infrastructure (such as the cloud) ensures that only authenticated users with the secret decryption key can access the data. For example, a smart thermostat that sends data to the operator must ensure the transmitted information remains protected and inaccessible to unauthorized parties.

Security Monitoring and Analysis: This involves capturing data from across the system, including endpoint devices and network traffic, to identify potential security violations. Once threats are detected, a range of security actions is triggered according to the overall system's security policy. Monitoring can be done in real-time or post- event, enabling the detection of multiple potential attack patterns. It is critical to secure endpoint devices from tampering and data manipulation.

Security Lifecycle Management: Lifecycle management enables service providers and OEMs to control the security of devices while they are operational. In the event of a cyber disaster, rapid over-the-air (OTA) device key replacement ensures minimal service disruption. Additionally, secure decommissioning of devices ensures that discarded devices cannot be repurposed or exploited to access services without authorization.

OPEN RESEARCH ISSUES

Smart homes have garnered significant attention in recent years, with many challenges and issues being identified. While substantial progress has been made, several areas still require improvement. Some issues are critical, while others have been somewhat addressed but still demand further exploration. Below are some open research issues that need more focused attention [49][50]:

Transformation of Conventional Homes to Smart Homes: A major challenge lies in converting traditional homes into smart homes with minimal cost and design alterations. Upgrading a house to a smart home often requires extensive modifications, from sensors to appliances. Smart appliances tend to be costly, which makes them unaffordable for many consumers. Current research lacks reasonable solutions to this problem, with many suggesting that smart homes should be built from scratch due to the substantial physical changes involved.

Interoperability Between Different Brands: Different manufacturers create smart devices based on varying standards, leading to significant interoperability issues. Although some global standards have been developed, the problem persists, especially when consumers purchase products from different manufacturers. These inconsistencies result in integration difficulties and operational issues across diverse devices, undermining the seamless functioning of smart homes.

Inflexibility of Systems: Many smart home systems and equipment come with pre-installed functionalities that may not meet users' specific needs. Research shows that consumers often want more flexibility and personal control over applications. For instance, in a family, each person might want to watch their favorite TV show simultaneously. Structural changes to enable greater flexibility remain a significant barrier to the widespread adoption of home automation.

Energy Efficiency: Energy consumption remains a significant concern in smart homes, particularly regarding communication devices. The energy usage of various devices is directly tied to their performance, and while multiple communication protocols like ZigBee, Wi-Fi, and Bluetooth exist, each has its own advantages and limitations. This area requires more focused research to optimize energy efficiency and balance performance across different devices and protocols [51].

Security Challenges: As wireless technology continues to evolve, the security challenges associated with smart homes also grow. While there has been significant progress, current security measures remain insufficient. Key security concerns include authentication, denial-ofservice (DoS) attacks, data breaches, and identity theft. More robust solutions are required to ensure the safety and privacy of users within smart homes [52].

CONCLUSION

Smart homes are revolutionizing the way we live, bringing automation, security, and efficiency to modern urban spaces. As part of the broader vision of smart cities, these interconnected systems use IoT technologies to enhance daily life—whether it’s controlling lighting, monitoring energy consumption, or securing homes with advanced biometric authentication. While the benefits of smart homes are undeniable, their widespread adoption faces several challenges, including security vulnerabilities, interoperability issues, and high implementation costs. This paper explored the technological advancements in smart home automation, covering key applications, core components, and the evolving security landscape to ensure these systems remain safe and reliable. Despite remarkable progress, there are still open questions about how to integrate diverse devices seamlessly, strengthen data protection, and make smart home solutions more affordable and accessible. As technology continues to evolve, researchers and industry experts must address these challenges to create truly intelligent, secure, and adaptable living environments. The future of smart homes is promising, but its success hinges on balancing convenience with security and efficiency. By tackling these issues head-on, we can ensure that smart homes not only enhance urban living but also offer a safe, sustainable, and interconnected future for all.

REFERENCES

[1]Alkandari, A. Alhammadi, and A. Alghamdi, "Smart Cities: Survey," Journal of Advanced Computer Science and Technology Research, pp. 79-90, 2012.
[2]J. Bowerman, L. Smith, and A. Williams, "The Vision of a Smart City," 2000. [3]S.
Ijaz, H. Zubair, and A. U. Rehman, "Smart Cities: A Survey on Security Concerns,"
[4]International Journal of Advanced Computer Science and Applications, vol. 7, 2016.
[5]Brush, B. A. Myers, and E. G. Tarrant, "Home Automation in the Wild: Challenges and Opportunities."
[6] J. Jungwoo, S. M. Lee, and B. H. Cho, "Building an Integrated Service Management Platform for Ubiquitous Cities," 2011.
[7] P. Fragkiadakis, S. O. K. S. P. A. M. C. F. J. E. W. D. E. H. S. E. K. S. L., "Ubiquitous Robust Communications for Emergency Response Using Multi-Operator Heterogeneous Networks," EURASIP Journal on Wireless Communications and Networking, pp. 1-16, 2011.
[8] S. M. Shaheed, "Effective Smart Home System Based On Flexible Cost in Pakistan," in The Fourth HCT Information Technology Trends (ITT 2017), Dubai, 2017.
[9] P. Waghmare, "Survey on: Home Automation Systems," in International Conference on Trends in Electronics and Informatics ICEI, 2017.
[10] P. P. Gaikwad, R. K. Gaikwad, and S. S. Gaikwad, "A Survey Based on Smart Home System Using Internet-of-Things," in International Conference on Computation of Power, Energy, [11]Information and Communication, 2015.
[12] V. Yadav, A. M. S. S. B., "Smart Home Automation Using Virtue of IoT," in 2nd International Conference for Convergence in Technology (I2CT), 2017.
[13] M. Asadullah, I. A. R. S. M. F. A. B. U. M. I., "An Overview of Home Automation Systems," Peshawar.
[14] N. Komninos, S. K. A. D. I. G., "Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures," IEEE Communication Surveys & Tutorials, vol. 16, p. 1933, 2014.
[15]P. Mongkolwat, S. N. S. S. K. B., "IoT-based LED Lighting Control in Smart Home," in 2018 IEEE International Conference on Applied System Invention (ICASI), 2018.
[16] J. Margulies, T. G. L., "Garage Door Openers: An Internet of Things Case Study," IEEE Security Privacy, vol. 13, pp. 80-83, 2015.
[17] F. Shhadeh, A. E. S. N., "System Architecture for Smart Home Meter," in 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes Systems (IT-DREPS), 2017.
[18]"Applications of Smart Homes," Link Labs, 17 Mar. 2015. [Online]. Available: https://www.link-labs.com/blog/applications-of-home-automation. [Accessed: 16 Dec. 2018].
[19] K. Bing, A. G. B. R., "Design of an Internet of Things-based Smart Home System," in The 2nd International Conference on Intelligent Control and Information Processing, 2011.
[20] N. Jose, M. S. R. M., "The Best Home Automation Apps to Make Your Life Easier," [Online]. Available: https://www.thinklions.com/blog/best-home-automation-apps/#6_Samsung_SmartThings_A_Central_Hub_For_Home_Automation. [Accessed: 4 Dec. 2018].
[21]AlShu'eili, H. S. A. K., "Voice Recognition Based Wireless Home Automation System," in 4th International Conference On, Kuala Lumpur, 2011.
[22]S. Sen, A. K. M. F., "Design of an Intelligent Voice Controlled Home Automation System," [23]International Journal of Computer Applications, vol. 121, pp. 39-42, 2015.
[24]R. Piyare, K. K. D., "Internet of Things: Ubiquitous Home Control and Monitoring System Using Android-based Smartphone," International Journal of Internet of Things, vol. 2, pp. 5-11, 2013.
[25]"Smart Home Sensors," IBM, 2016. [Online]. Available: https://www.ibm.com/blogs/internet-of-things/sensors-smart-home/.

[26]R. Sharma, N. K., "Top 15 Sensor Types Being Used in IoT," [Online].
Availablehttps://www.finoit.com/blog/top-15-sensor-types-used-iot/.
[27]M. Kuzlu, S. A., "Review of Communication Technologies for Smart Homes/Building Applications," IEEE, 2015.
[28]F. Al-Turjman, R. B., "Small Cells in the Forthcoming 5G/IoT: Traffic."
[29]F. Vafa, H. H. P., "Wireless Sensor Networks and LTE-A," in IEEE 38th Conference On Local Computer, 2013.
[30]P. McDermott-Wells, J. W. F., "What is Bluetooth?," IEEE Potential, vol. 23, pp. 33-35, 2004. [31]S. Samuel, V. S. H., "A Review of Connectivity Challenges in IoT-Smart Home," in 3rd MEC International Conference on Big Data and Smart City (ICBDSC), 2016.
[32]S. Samuel, K. A. N., "A Review of Connectivity Challenges in IoT-Smart Home," in 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), 2016.
[33]"Authentication Hacking: What are Authentication Hacking Attacks?," Acunetix, [Online].
Available: https://www.acunetix.com/websitesecurity/authentication/. [Accessed: 21 Dec. 2018].
[34]H. Liu, F. T. M., "Smart Solution, Poor Protection," in IoT S&P'1, Dallas, TX, USA, 2017. [35]P. L. R. Chze, S. M. T., "Secured IoT Gateway For Smart Nation Applications," in 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, 2018.
[36]J. Y. Kim, S. Y. K., "Smart Home Web of Objects-based IoT Management Model and Methods for Home Data Mining," in 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2015.
[37]H. Zheng, S. M., "Modeling and Analysis of ZigBee-Based Smart Home System," in 5th International Conference on Digital Home, 2014.
[38]C., S. K., "Autonomic Computing Through Reuse of Variability Models at Runtime: The Case of Smart Homes," Computer, vol. 42, pp. 37-43, 2009.
[39]J. H., A. T., "Security Considerations for Secure and Trustworthy Smart Home System in the IoT Environment," in 2015 International Conference on Information and Communication Technology Convergence (ICTC), 2015.
[40]D., N. T., "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017.
[41]N. Komninos, F. G., "Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures," IEEE Commun. Surv. Tutorials, vol. 16, no. 2014, pp. 1933-1954, 2014.
[42]R. R., S. N., "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," Computer Networks, vol. 57, no. 2013, pp. 2266-2279, 2013.
[43]M. G., A. A., "Special Issue on the Theory and Practice of Differential Privacy," 2017.
[44]J. Y. Kim, A. Y. S., "Smart Home Web of Objects-based IoT Management Model and Methods for Home Data Mining," in 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2015, pp. 327-331.
[45]H. Z., F. K., "Modeling and Analysis of ZigBee-Based Smart Home System," in 2014 5th International Conference on Digital Home, 2014, pp. 242-245.
[46]Tyagi, A. K., Gupta, M., Aswathy, S. U., & Ved, C. (2021). Healthcare solutions for smart era: An useful explanation from user's perspective. Recent trends in blockchain for information systems security and privacy, 9781003139737-13.

[47]Gupta, M., Ved, C., & Kumari, M. (2022). Emergence of Blockchain Applications with the 6G-Enabled IoT-Based Smart City. In Blockchain for 6G-Enabled Network-Based Applications (pp. 213235). CRC Press.
[48]Alazab, M., Gupta, M., & Ahmed, S. (2023). AIoT technologies and applications for smart environments. Institution of Engineering and Technology.
[49]Gupta, M., Kumar, R., Larhgotra, A., & Ved, C. (2023). Emergence of Big Data and Blockchain Technology in Smart City. In Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities (pp. 83-101). CRC Press.
[50]Bansal, D., Bansal, M., Tharani, K., Gupta, M., Goyal, B., & Dogra, A. (2022, October). Enhancement of smart grid technology using end-to-end reinforcement learning in deep q- network. In AIP Conference Proceedings (Vol. 2555, No. 1). AIP Publishing.
[51]Kumar, A., Jain, R., Gupta, M., & Islam, S. M. (Eds.). (2023). 6G-enabled IoT and AI for smart healthcare: challenges, impact, and analysis. CRC Pres

IoT for Real-Time Pest Detection in Agriculture

[1]Prachi Nalawade, [2]Harsh Singanjude, [3] Sudeepta Banerjee

1,2 Student, Master of Computer Application (MCA), MIT WPU, Pune, INDIA
3Professor, School of Business, MIT WPU, Pune, INDIA
2Corresponding Author: singanjudeharsh@gmail.com

ABSTRACT

The increasing prevalence of pests poses a significant challenge to agricultural productivity, often leading to reduced yields and economic losses for farmers. Traditional pest detection methods are often reactive, labour-intensive, and inefficient, making it difficult to implement timely interventions. This research explores the potential of the Internet of Things (IoT) to revolutionize pest detection by enabling real-time monitoring and analysis in agricultural environments. By deploying IoT-enabled sensors, cameras, and data analytics platforms, farmers can receive accurate, real-time insights into pest activity, environmental conditions, and crop health. The study focuses on integrating advanced technologies such as machine learning algorithms, wireless sensor networks, and cloud computing to create a robust and scalable pest detection system. This approach not only enhances the accuracy of pest identification but also supports predictive modelling to anticipate pest outbreaks. The research also examines the economic and practical feasibility of IoT deployment in small-scale and resource-limited farming setups, ensuring inclusivity and scalability. By combining real-time data acquisition with actionable insights, this IoT-based solution aims to empower farmers to implement timely, targeted pest control measures, ultimately reducing chemical pesticide usage, minimizing crop damage, and promoting sustainable farming practices. This paper highlights the design, development, and field evaluation of the proposed system, along with its potential implications for the future of precision agriculture.

1. INTRODUCTION

Agricultural production has long been engaged in pest control, with an immediate relationship to crop yield, food quality, and farm profitability. Traditional measures of pest management have included massive pesticide application, increasing expenditure, environmental degradation, and human risk. With an increasing demand for food worldwide and environmental stress, cost-effective and environmentally sound practices of pest management are urgently needed.

In the last ten years, the IoT has transformed various sectors of the economy, including agriculture. IoT is made possible by integrating sensors, networks of communication, and data analysis, facilitating real-time monitoring and decision- making, and offers scope for more precise and specific interventions. Its various applications in agriculture, such as IoT in real-time pest detection, are a groundbreaking attempt to address the requirements of pest management.

This research explores the potential of IoT-based systems to monitor and control pests in farm fields. Through a network of sensors and cameras, these systems warn farmers before pest infestation, which can allow for early intervention and reduction in the application of lethal chemical pesticides. The IoT systems may also incorporate predictive analytics, wherein preventive actions to control pests are implemented based on real-time inputs and weather conditions.

The main purpose of this research is to validate the efficacy, useability, and effect of IoT in the real-time detection of pests in agriculture. This entails confirming its capability to enhance production of crops, lower the utilization of pesticides, enhance profitability at the farm gate, and enhance sustainable agriculture. Through this research, we are hoping to demonstrate how IoT can transform the way pests are managed such that it will be more efficient, eco-friendly, and affordable for farmers all over the world.

2. LITERATURE REVIEW

Internet of Things (IoT) deployment in the agriculture sector has been one of the top themes of the past years, with the theme of precision and sustainability being paramount. Its actual-time applications in the identification of pests is one of the widening areas of research under such paradigms. It is under such an atmosphere that some of the primary findings and research papers that constitute the foundation for the deployment of IoT to detect pests have been showcased.

2.1. Evolution of IoT in Agriculture

IoT technologies have revolutionized the agriculture industry by providing automation, decisionmaking based on data, and real-time tracking. Monitoring of soil moisture, weather prediction, and crop disease management were a few of the first IoT uses in agriculture. Studies by Zhang et al. (2017) and Ahmed et al. (2019) enumerated the use of IoT devices like sensors and drones to monitor environmental factors, which impacted pest management indirectly. These general applications led to specialized applications, i.e., for pest detection.

2.2. Advances in Pest Detection Technologies

Before the dawn of IoT, pest detection had been a cumbersome and human-error- susceptible activity on the basis of manual observation and static traps. But after the dawn of IoT, scientists oriented towards the usage of automated systems for detecting pests. A key research work on this area includes that of Kumar et al. (2020), wherein image-based detection mechanisms were used with IoT networks in order to detect particular pests infesting crops. Accordingly, Choudhury et al. (2021) developed sensor-based systems that monitored temperature and humidity variations, which are normally common with pest infestation. However, the systems were plagued with scalability and real-time processing issues.

In **Machine Learning** and Artificial Intelligence for Pest Detection Accuracy and performance in detecting pests have also been enhanced through artificial intelligence (AI) and machine learning (ML). Sharma et al. (2022) presented an example of applying convolutional neural networks (CNNs) to distinguish between pests from pictures taken by IoT cameras. The method enhanced detection accuracy even with varying light and environmental conditions. Others, such as Li et al. (2020), constructed prediction models based on the past and actual data in an attempt to forecast the activity of the pest infestations and thereby conduct the interventions accordingly. Integration of Wireless Sensor Networks and IoT Wireless Sensor Networks (WSNs) have been exploited extensively in IoT to collect and transport data. Patel et al. (2018) within their study enumerated utilization of WSNs towards creating networked systems that can be used in monitoring large- scale agriculture farms. Seamless communication was ensured between cameras, sensors, and cloud platforms through the networks. Network latency and

power efficacy are still foremost bottlenecks for large-scale deployment. Economic and Practical Implications Use of IoT in agriculture, especially for pest monitoring, has been controversial on cost and sustainability to poor farmers. Fernandez et al. (2019) and Gupta et al. (2020) conducted research on low-cost IoT configurations with solar-powered sensors and open-source platforms to lower the cost of the systems. The research focused on the requirement for solutions that are optimized for poor-resource environments. Ethical and Environmental Implications Among the major benefits of pest identification using IoT is reducing the application of chemical pesticides. Singh et al. (2021) also stated the eco-friendly advantage of precision pest management, like avoids pesticide seepage into water bodies. Ethical implications of data ownership and privacy issues in IoT technologies were also identified by scholars such as Johnson and Wang (2022), who presented models of secure and open data sharing.

Research Gaps and Directions Despite the available development, there are gaps in literature. Scalability and long-term stability of the current systems are mainly constrained in dynamic Agri-environments. In addition, IoT with predictive analytics integration has not yet been leveraged to the best degree. These gaps need to be addressed by future research, particularly by the establishment of energy-efficient IoT devices and data interoperability. Lastly, existing literature provides a backdrop for IoT to enable real-time pest detection innovations. Still, integrative and scalable solutions with advanced analytics that incorporate IoT as a primary component are miserably lagging and massively in immediate need among farmers across the world. This research contribution will bridge such shortcomings with an effective IoT-based solution for real-time pest detection and management.

3. IMPACT ON AGRICULTURE Environmental Impact

Reduced Pesticide Use : Traditional pest management is typified by indiscriminate spraying of pesticides across the entire field, resulting in excessive chemical application, environmental contamination, and harm to non-target organisms. The affected fields can be treated separately by farmers through IoT- based pest sensing, thus reducing the overall application of pesticides. This means healthier environments, reduced water pollution, and better soil quality.

Economic Impacts

Low Costs : Because IoT is utilized in the identification of the pests, farmers can act accordingly, e.g., spraying the pesticides where there are pests, hence minimizing procurement expenses of pesticides, labour, and application equipment. Identification of the pests at the right time also avoids the devastation of the crops, hence reduction of loss and increase in profitability.

Increased Yields: Early detection of pests by farmers and their immediate action ensures that the farmers do not allow mass destruction of crops. This translates to increased yields and quality of crops, which contributes to the economic value as a whole. Effective control of pests at the right time also translates to farmers not having to suffer complete loss of crops, whose effects can be cripplingly devastating on the economy.

Angled Operational Efficiency: Since it is the duty of IoT sensors to identify the pests and instantly send out notices, farmers are exempted from the time that is spent manually inspecting. This translates into better farm operations management. Also, automated devices can assist in scheduling pest control operations, which exempts human labor from working round the clock. Climate Change Mitigation.

Adaptation to Climate Variability: As climate change influences the activity and pattern of pests, IoT can enable farmers to adjust real-time based on pest movement and infestation. By observing the trend of the change in activity of the pest, farmers can prepare and take action to reduce the impact of climate change on yields.

4. CONCLUSION

This study investigated the use of IoT for Real-Time Pest Detection in Agriculture, which can transform pest control with a greener, more efficient, and cost-effective option for existing methods. Farmers are enabled by using an IoT sensor network, cameras, and analytics to detect and respond to infestations of pests early, minimize the use of pesticides, lower environmental impact, and optimize utilization of resources. The research confirmed that IoT-based pest detection systems can be simply amazing in all aspects of agriculture. They are: Improved Pest Control: Early detection at the initial stage and specific pest control measures minimize crop loss and pest infestation. Decrease in Chemical and Pest Control Costs: Farmers refrain from using chemicals utilized and pest control and utilize it only when necessary, thus decreasing their operating expenses.

Environmental Sustainability: As pesticides decline, the agricultural environmental impact is reduced, resulting in improved environments and biodiversity. Increased Productivity: Improved pest management and more efficient pest management processes mean more production and higher quality produce. The study also highlights the need for data-driven decision-making in contemporary agriculture. The combination of IoT with machine learning and predictive analytics generates actionable insights for farmers that enable them to develop proactive pest control measures. It not only helps farms become profitable but also ensures farming practices' sustainability in the long run.

However, there were some problems that were faced, including the cost of initial investment, network dependability, and educating and training farmers on IoT technology. It will be essential to overcome these problems in order to make it more acceptable at a broader level, particularly for poor and small-scale farmers. In summary, IoT can revolutionize pest control activities in agriculture. With technology innovation and affordability, large-scale deployment of IoT to track pests in real-time can lead to more efficient, sustainable, and profitable farming. Additional research must be carried out in a bid to simplify system designs, lower costs, and expand the deployment of IoT solutions in an attempt to maximize their contribution to agriculture in the world.

REFERENCES

[1] Zhang, L., & Liu, H. (2017). "IoT-Based Systems for Precision Agriculture: A Review." *Journal of Agricultural Technologies*, 12(3), 45-58.

[2] Ahmed, S., & Banerjee, T. (2019). "Environmental Monitoring in Agriculture Using IoT Devices." *Computers in Agriculture*, 8(4), 123-136.

[3] Kumar, R., & Sharma, A. (2020). "IoT-Integrated Image-Based Pest Detection Systems: Challenges and Opportunities." *Sensors and Applications*, 15(6), 234-245.

[4] Choudhury, P., & Roy, D. (2021). "Humidity and Temperature-Based Pest Detection Using IoT Sensors." *International Journal of Agricultural Informatics*, 9(1), 89-101.

[5] Sharma, M., & Gupta, V. (2022). "Machine Learning for Pest Detection: Applications and Case Studies." *AI in Agriculture*, 7(2), 101-115.

[6] Li, J., & Wang, Y. (2020). "Predictive Modeling of Pest Outbreaks Using IoT and Historical Data." *Smart Farming Systems*, 14(5), 67-79.

[7] Patel, K., & Mehta, S. (2018). "Wireless Sensor Networks in Agriculture: A Comprehensive Study." *IoT Journal*, 10(4), 203-217.

[8] Fernandez, A., & Lopez, R. (2019). "Affordable IoT Solutions for Small-Scale Farmers." *Rural Technology Advances*, 6(3), 12-22.

[9] Gupta, N., & Arora, S. (2020). "Open-Source IoT Platforms for Resource- Constrained Agriculture." *Journal of Agricultural Innovation*, 11(2), 45-58.

[10] Singh, R., & Kaur, P. (2021). "Targeted Pest Control with IoT: Environmental Benefits and Challenges." *Environmental Science in Agriculture*, 18(7), 76- 88.

[11] Johnson, K., & Wang, L. (2022). "Data Privacy and Ownership in IoT-Enabled Agriculture Systems." *Cybersecurity and Ethics in Technology*, 5(1), 34-49.

Distributed Mobile Cloud Computing Services

Ramiz Salama[1*], Fadi Al-Turjman[2, 3]

[1]*Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University Nicosia, Mersin 10, Turkey*
[2]*Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute, Near East University, Nicosia, Mersin10, Turkey*
[3]*Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey*
**Corresponding author Email: ramiz.salama@neu.edu.tr*

ABSTRACT

The advantages of cloud computing and mobile computing are combined in mobile cloud computing (MCC), which provides mobile devices with ubiquitous access to services, increased processing power, and storage capacity. In conventional cloud computing models, mobile devices use the internet to access centralized cloud resources. However, centralized systems have limitations in terms of responsiveness and efficiency as mobile apps become more complex and require real-time processing, faster performance, and lower latency. In response to these issues, a paradigm known as Distributed Mobile Cloud Computing (DMCC) has surfaced, in which cloud resources are dispersed over several sites, frequently nearer to the end users. This distributed architecture optimizes bandwidth utilization, lowers latency, and improves service availability by offloading processing activities from mobile devices via edge computing, fog computing, and cloudlets. DMCC makes it possible for resource-intensive applications to function well on mobile platforms, including augmented reality (AR), real-time data analytics, and sophisticated biometric authentication. Scalability, fault tolerance, and energy efficiency are promoted by the architecture's distribution of computational activities over a network of nearby and distant cloud resources. But it also brings with it additional difficulties including system complexity, effective resource allocation, and security threats. The basic ideas, design, and uses of distributed mobile cloud computing services are covered in this paper. It highlights the potential of DMCC to transform next-generation mobile applications and services by examining important technological issues and providing insights into new solutions.

Keywords: cloud computing, cloud computing services, and mobile cloud computing

1. INTRODUCTION

Numerous modeling techniques, including as software as a service, online storefronts, community networks, and cloud computing, have been developed as a result of advancements in network- based computing. By offering remote access to material and apps, cloud computing enables third- party providers to offer services from any location, at any time, and in a variety of circumstances. A pay-per-use service, cloud computing offers software, memory, processing power, and storage as needed. Data centers, virtualization, and on-demand computing are its three main technologies.

Resource consumption is optimized by task dispersion. Mobile Cloud Computing, which centralizes computers and services for clients, has arisen with the popularity of smartphones. Distributed computing systems can be built using mobile devices, where each node is specified by a wireless communication architecture and a device [1–3]. As a result, Mobile Cloud Computing (MCC) has become popular, overcoming the limitations of mobile devices in terms of processing, storage, and networking. The main strategies for distributed cloud computing, important characteristics, and important mobile cloud computing technologies are covered in this review study.

2. Models for Cloud Deployment

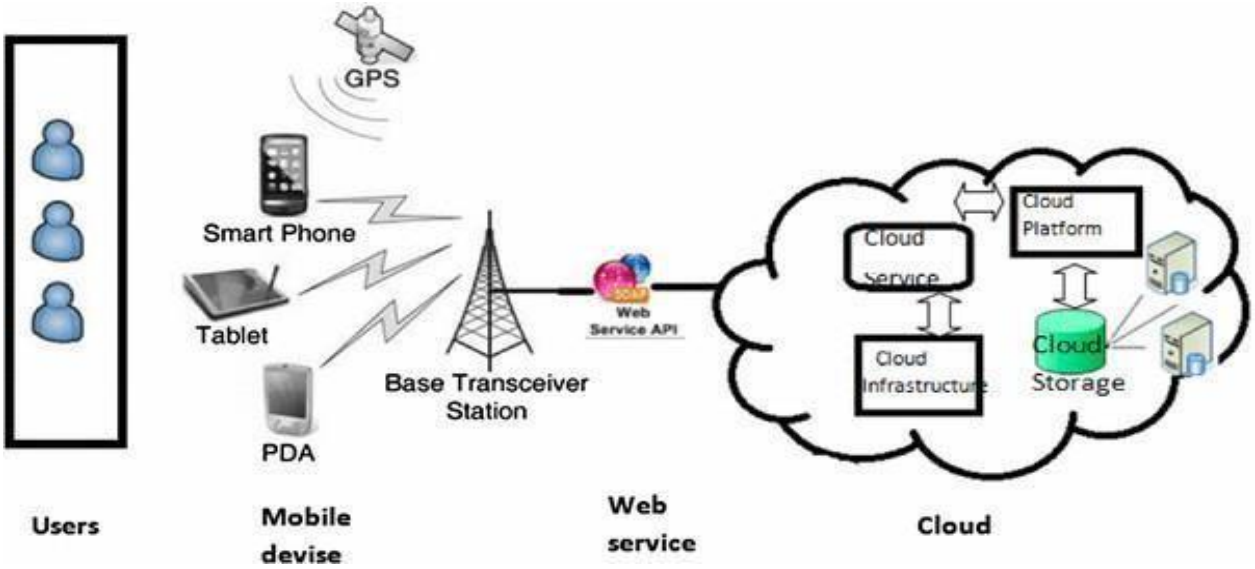


Figure1 Mobile Cloud Computing

Different application models based on service models can be implemented using cloud computing; Kumari and Singh (2021) have identified four main ones.

1) Private clouds provide improved data security, flexibility, scalability, and dependability and are customized for specific businesses or organizations.

2) Because of their widespread accessibility and suitability for storing non-sensitive data, public clouds which are run by hosting companies offer shared resource pools for service delivery, raising security concerns.

3) Deploying a community cloud entails sharing cloud infrastructure across several organizations in the community. This enables cooperative management by the community or a cloud service provider and permits remote access to stored files.

4) Hybrid cloud architecture combines public and private clouds to store data while preserving their unique identities for different deployment circumstances.

3. MODELS OF CLOUD COMPUTING SERVICES

With three tiers according to capacity and service provider model, cloud computing leverages computers, hardware, and networks to provide services. Customers may control components like operating systems and applications without having to worry about infrastructure upkeep thanks to Infrastructure as a Service (IaaS), which offers virtual computing resources like virtual machines. Using programming languages, resources, and tools that the cloud operator provides, PaaS is an internet-based platform for creating and sharing technologies and applications. By providing computer language libraries and tools for the development and deployment of applications, it makes software development easier. SaaS is a type of software delivery in which users obtain software over the cloud. Grid computing, parallel computing, and distributed computing are all included in cloud computing. For effective workload allocation, load balancing is essential. Cost reduction, geo-replication, redundancy, and dependability are all benefits of distributed cloud computing. It enhances data localization while reducing expenses and overheads associated with connectivity. Effective management of user needs requires efficient resource allocation [4–10]. Concerns about latency have led to the adoption of distributed clouds, particularly in data center-intensive scenarios such as cooperative document editing or gaming, where local clients include computers, robots, self-driving cars, and humans.

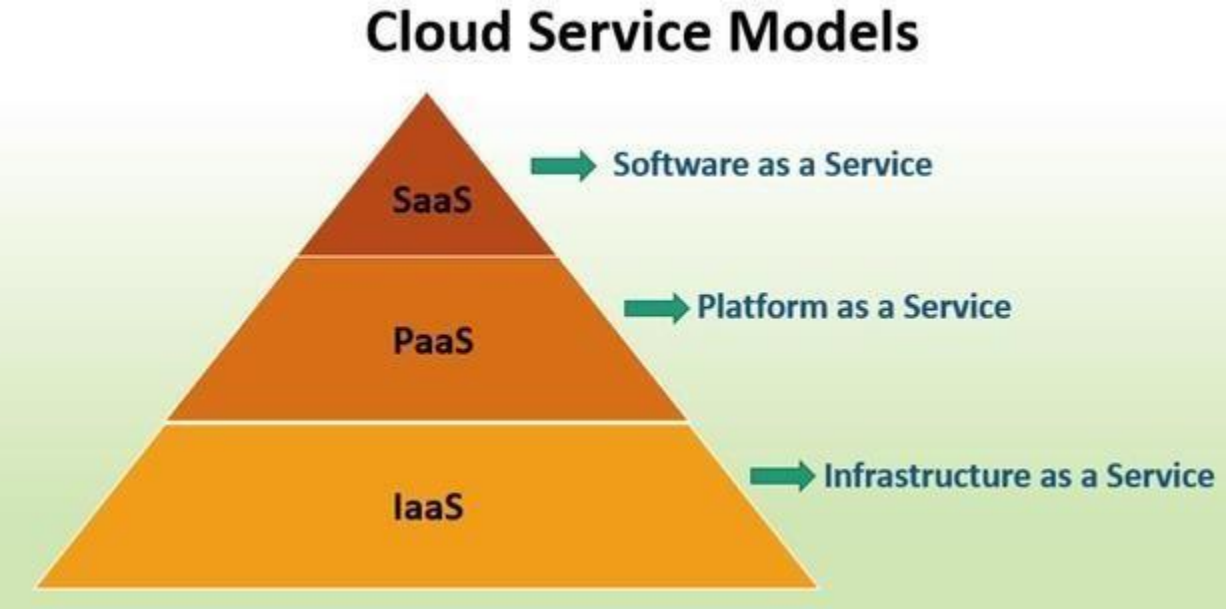


Figure 2. Cloud Service Models

4. MOBILE CLOUD COMPUTING

Thanks to developments in networking, wireless technology, and mobile computing, the number of mobile users has increased dramatically, producing enormous amounts of data globally. The need for workplace mobility and the widespread use of sensors in mobile devices have led to the growth of mobile cloud computing, or MCC. In order to handle resource limitations in cellphones, MCC combines wireless networks, cloud computing, and mobile computing to manage and analyze data. Because wireless communication lines are vulnerable, mobile cloud computing (MCC) poses security risks. New privacy-conscious authentication techniques are required to

counter this. Cloud computing and mobile devices must be integrated to optimize capabilities and overcome smartphone constraints. It is crucial to comprehend these traits in order to conduct additional study and development [11].

5. ARCHITECTURE FOR MOBILE CLOUD COMPUTING

Because of their many uses, mobile devices are becoming more and more commonplace in daily life. However, their designers must contend with resource limitations, such as limited CPU power and storage space. In order to get over these restrictions, Mobile Cloud computer (MCC) makes use of external computer resources. In the MCC architecture, tasks are carried out by mobile devices interacting with networking base stations. Because MCC architectural models include service-oriented architecture (SOA) layers, security considerations are essential. While the internet service layer links the mobile network to the cloud through fast connections, the mobile network layer links mobile users to cloud services through devices like smartphones and tablets [12]. A layer of cloud computing services provided by several service providers is known as the Cloud Services Provider Layer (MCC). It discusses smartphone processor power, storage capacity, battery life, and hardware constraints. MCC is crucial for contemporary mobile computing environments because it addresses hardware constraints and maximizes external computing resources.

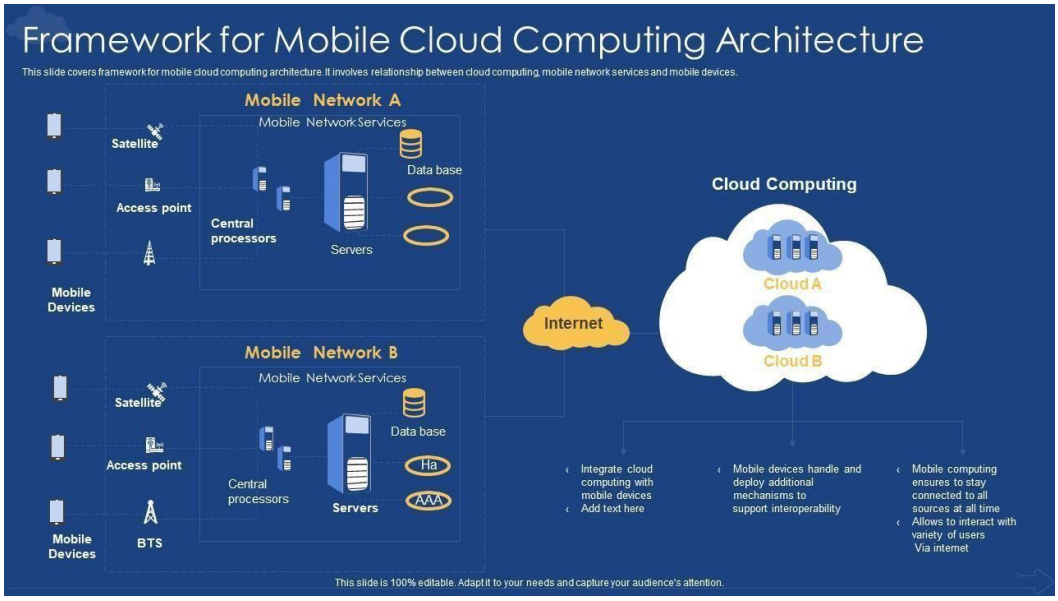


Figure 3. Mobile Cloud Computing Architecture

6. MOBILE CLOUD COMPUTING'S ADVANTAGES

Mobile cloud computing (MCC) is a valuable architecture that provides end users and enterprises with several advantages, such as simplicity of infrastructure construction and maintenance.

1. *Improving Battery Lifetime:* By shifting data processing and storage responsibilities to the cloud, especially for resource-intensive tasks that can rapidly drain the battery when carried out locally, MCC increases device battery life.
2. *Storage:* Cloud storage provides infinite capacity, removing the need to invest in server infrastructure and space issues, and lowering IT expenses related to hardware updates and maintenance for businesses.
3. *Improving Processing Power:* Applications that demand a lot of processing power, such as transcoding, gaming, and multimedia streaming, benefit from MCC's cloud-based processing capabilities.
4. *Disaster Recovery and Backup:* Unlike traditional physical storage solutions, cloud computing providers offer comprehensive backup and recovery services that streamline data backup and *restoration procedures and improve disaster recovery capabilities.*
5. *Scalability:* By allowing for scalability across web, cloud, and mobile devices, mobile apps can adjust to shifting user needs and meet different usage patterns.
6. *Reliability:* Cloud infrastructure outperforms individual devices in terms of security features like virus detection and authentication, guaranteeing the dependability and safety of cloud-based apps.

Beyond individual users, mobile cloud computing has a host of advantages for enterprises, such as improved performance, scalability, security, and dependability [13-30].

7. **Actual life uses for mobile cloud computing services that are dispersed.**

In order to increase speed, prolong battery life, and provide scalable, real-time services, distributed mobile cloud computing, or DMCC, combines mobile devices with cloud computing infrastructure. Distributed mobile cloud computing services have several practical uses, such as:

1. Smart Cities

- Traffic Management: By combining data from dispersed mobile devices, including smartphones, sensors, and cameras, DMCC assists in real-time traffic pattern analysis, improving traffic flow, and easing congestion.
- Environmental Monitoring: Temperature, noise levels, and air quality are measured by dispersed mobile sensors, which then process and analyze the data in the cloud. This enhances public health and encourages responsible environmental management.

2. Medical Care and Telemedicine

- Remote Monitoring: To provide ongoing health monitoring and prompt interventions, wearable technology and smartphone apps gather health data, including heart rate and blood sugar levels, which is then processed in the cloud.
- Medical Image Processing: Distributed clouds can process large medical pictures, such CT and MRI scans, giving clinician's remote access to improved diagnostic tools.

3. Augmented Reality (AR) and Virtual Reality (VR)

- Gaming and Entertainment: By shifting processing from mobile devices to cloud servers, DMCC enables resource-intensive AR/VR apps, providing immersive experiences while lowering latency and preserving responsiveness.

• Education and Training: To scale and provide low-latency experiences on mobile devices, AR/VR apps for remote learning and simulation-based training make use of distributed cloud computing.

4. Social Networks on the Go

• Content Sharing: Distributed mobile cloud computing eases the load on individual devices by processing and storing large volumes of images, videos, and other content in social media apps, allowing for rapid access to the media.

• Personalized Content Delivery: By analyzing user behavior and preferences, cloud services improve user experience by instantly delivering personalized content to mobile users.

5. IoT and Edge Computing

• Smart Homes: By shifting data processing to cloud infrastructure, distributed mobile clouds improve automation and efficiency by enabling real-time control of IoT devices (such as smart lights, thermostats, and security systems) through mobile apps.

• Industrial IoT (IIoT): DMCC analyzes data from dispersed sensors in manufacturing facilities to provide predictive maintenance and real-time monitoring, minimizing downtime and enhancing operational effectiveness.

6. MVNOs, or mobile virtual network operators

• Flexible Network Management: By using DMCC services to flexibly distribute network resources, MVNOs can provide scalable and reasonably priced mobile communication services in response to real-time demand, thereby enhancing user service quality.

7. Mobile Apps for Collaboration

• Crowdsourcing Platforms: Distributed mobile cloud computing is used by mobile apps that rely on user-generated content, like Waze (traffic data) or OpenStreetMap, to process and integrate data from multiple mobile devices and provide users with accurate and timely information.

• Distributed Computing Projects: Apps such as SETI@home work with cloud services to do distributed computing tasks for research objectives by utilizing the idle processing power of mobile devices.

8. Mobile Cloud Gaming

• Game Streaming: By shifting processing and graphics rendering to robust cloud servers, DMCC allows cloud gaming platforms such as Google Stadia or Xbox Cloud Gaming to stream top-notch games to mobile devices while maintaining a fluid gameplay experience with low latency.

9. Retail and E-Commerce

• Mobile Payment Systems: By processing transactions in the cloud while upholding high security and low latency replies, DMCC guarantees the security and scalability of mobile payment apps (such as Apple Pay and Google Pay).

• Inventory Management: By processing and analyzing data in the cloud, retailers may optimize supply chain management and stock levels while managing inventory in real time across numerous stores using distributed mobile cloud computing.

These uses demonstrate how DMCC aids in resolving issues with scalability, throughput, and real-time data processing in a variety of sectors.

1. The potential applications of dispersed mobile cloud computing services.

A model known as Distributed Mobile Cloud Computing (DMCC) makes use of cloud computing resources dispersed among numerous mobile devices and edge servers. As it improves computing efficiency, latency, and resource usage by bridging the gap between cloud services and mobile devices, its potential is enormous. The following are some crucial areas for possible development:

1. Integration of 5G and Edge Computing

- Applications with Low Latency: By lowering latency and processing data closer to the edge, DMCC in conjunction with 5G networks makes real-time applications possible, such as driverless vehicles, virtual reality, and augmented reality.
- Decentralized AI: More individualized and contextually aware AI systems can be produced by training and running AI models on dispersed devices.

2. Smart Cities and IoT

- Real-Time Data Processing: DMCC will enable local data processing by Internet of Things (IoT) devices in smart cities, as well as the sharing of pertinent data with the cloud for more comprehensive analytics. Better trash management, energy saving, and traffic systems will result from this.
- Improved Scalability: As the number of connected devices increases, distributed mobile clouds will enable the smart city infrastructure's quick scalability, enabling more effective resource management.

3. Efficiency in Energy Use

- Resource Optimization: By shifting computation-intensive jobs to dispersed clouds, mobile devices' energy usage can be optimized. The requirement for high-power computation on individual devices is decreased when workload is distributed evenly among devices, increasing overall system efficiency.
- Green Cloud Computing: By leveraging local computing resources, distributed mobile cloud computing can result in more energy-efficient systems by lowering data transit and, consequently, energy consumption in comparison to centralized cloud models.

4. Wearable technology and healthcare

- Telemedicine: By processing patient data from wearables and mobile sensors in real-time, mobile cloud computing may be essential to telemedicine, allowing for remote monitoring and quicker diagnosis.
- Distributed Health Data Management: By using edge computing to protect patient privacy, DMCC may enable distributed health records management, guaranteeing quicker access to patient data.

5. Security and Privacy of Data

- Decentralized Data Control: By integrating blockchain technology, DMCC can enhance data security and privacy by enabling decentralized data storage and access control systems, particularly in delicate industries like healthcare and finance.

- Distributed Security Models: By lowering single points of failure, security procedures can be dispersed among nodes, increasing resistance to cyberattacks.

6. Virtual and Augmented Reality

- Real-Time Processing: By utilizing distributed mobile and edge resources, DMCC will make it possible for AR and VR apps to process data in real time. As a result, applications for leisure, education, and gaming will run more smoothly.
- Less Network Congestion: By shifting AR/VR data processing to the dispersed mobile cloud, centralized servers will be less taxed, allowing for quicker and more scalable content delivery.

7. Autonomous Systems

- Drones and Autonomous Vehicles: By processing data on edge nodes and neighboring devices, distributed mobile cloud services may allow autonomous systems, such as drones and self-driving automobiles, to make decisions more quickly.
- Collaborative Learning: Distributed learning models, in which drones and cars share real-time information, can help autonomous systems by eliminating the requirement for all processing to take place in central cloud data centers.

8. Gaming and Entertainment

- Cloud Gaming: With DMCC guaranteeing quicker reaction times, reduced latency, and improved user experiences, there will be a rise in demand for cloud gaming services. Workloads related to gaming could be transferred from mobile devices to dispersed cloud nodes.
- Streaming Services: By shifting processing duties to the edge, lowering latency, and delivering high-quality video, DMCC will maximize video streaming, particularly in areas with inadequate internet access.

9. Business and Enterprise Applications

• Mobile Enterprise Solutions: Companies will use DMCC more and more for remote and mobile workforce management, giving workers safe, effective access to cloud resources from any location. • Distributed Workflows: By distributing cloud services over several servers and mobile devices, enterprises can manage intricate workflows more effectively, increasing output and decreasing downtime.

10. Environmental Monitoring

Distributed Sensor Networks: Using IoT sensors dispersed throughout various places, mobile cloud computing may be utilized to monitor environmental variables in real time, such as water levels and air quality. Faster decision-making in disaster relief and climate change monitoring will be made possible by this.

11. Decentralized Finance (DeFi) and Blockchain

- Mobile Blockchain Nodes: By enabling mobile devices to function as nodes in a decentralized network, DMCC might facilitate blockchain applications by facilitating data sharing, smart contracts, and quicker and more secure financial transactions.

• Distributed Ledger Technology: By combining DMCC with distributed ledger technology, government operations, healthcare data, and financial institutions may become more transparent and secure.

12. Social Networks of the Next Generation

• Localized Content Sharing: By facilitating localized data processing and content sharing, improving privacy, and lessening the strain on centralized servers, DMCC can aid in the development of next-generation social networking platforms [45].

• Context-Aware Communication: By using DMCC, social networks can provide notifications and material in a way that is more contextually aware of the user's current surroundings and device capabilities [46].

Because of the increasing reliance on mobile devices, edge computing, the Internet of Things, and cloud infrastructure, distributed mobile cloud computing has a bright future with enormous potential across numerous industries. This paradigm, which offers improved performance, scalability, and sustainability, will influence technology in the future.

Figure 4. Future of Cloud Computing

9. CONVERSATION

Applications and data are integrated across regional borders by cloud computing, and distributed cloud computing makes collaborative workflows possible. No matter where they are, users can access computational resources using mobile cloud computing [43], facilitating sophisticated data

processing and rich multimedia experiences. The combination of cloud and mobile technology [44] spurs innovation across sectors and breaks down conventional barriers.

In cloud computing and mobile technology, load balancing is essential for maximizing efficiency and resource use. It optimizes power usage, increasing efficiency and prolonging the life of mobile devices. Modern computing paradigms are centered on the pursuit of scalability, with distributed and mobile cloud computing spearheading the movement toward adaptable computation and a more robust digital infrastructure [31-40].

Numerous advantages of distributed and mobile cloud computing include changing user interactions, spurring innovation in a variety of fields, and quickening the convergence of mobile and cloud technology [41] [42].

Table (1): Summary of Distributed Cloud Computing.

Feature	(Z. A. S. A. et al Najat Z, 2019)	(Miguel Castanheira Sanches, n.d.)	(Salem, n.d.)
process a batch or a stream of data		✓	
support scalability		✓	
reduced latency times	✓	✓	
achieve high performance			
high resource utilization			
performing huge processing	✓		✓
utilizing power via cloud domain	✓	✓	
reduce a huge amount of processing power	✓	✓	✓

Table (2). Summary of Mobile Cloud Computing

Feature	(He et al., 2018)	(Z. A. S. A. et al Najat Z, 2019)	(Borcea et al., n.d.)	(Salem, n.d.)	(Mishra et al., n.d.)
solve a long-standing problem			✓		
identity-based signature scheme	✓				
less computation time	✓				
Fewer communication costs	✓				
parallel computations	✓	✓			
better performance	✓	✓			
power saving		✓			
Improve performance		✓		✓	
Huge Computation saving				✓	
Increasing Scalability					✓

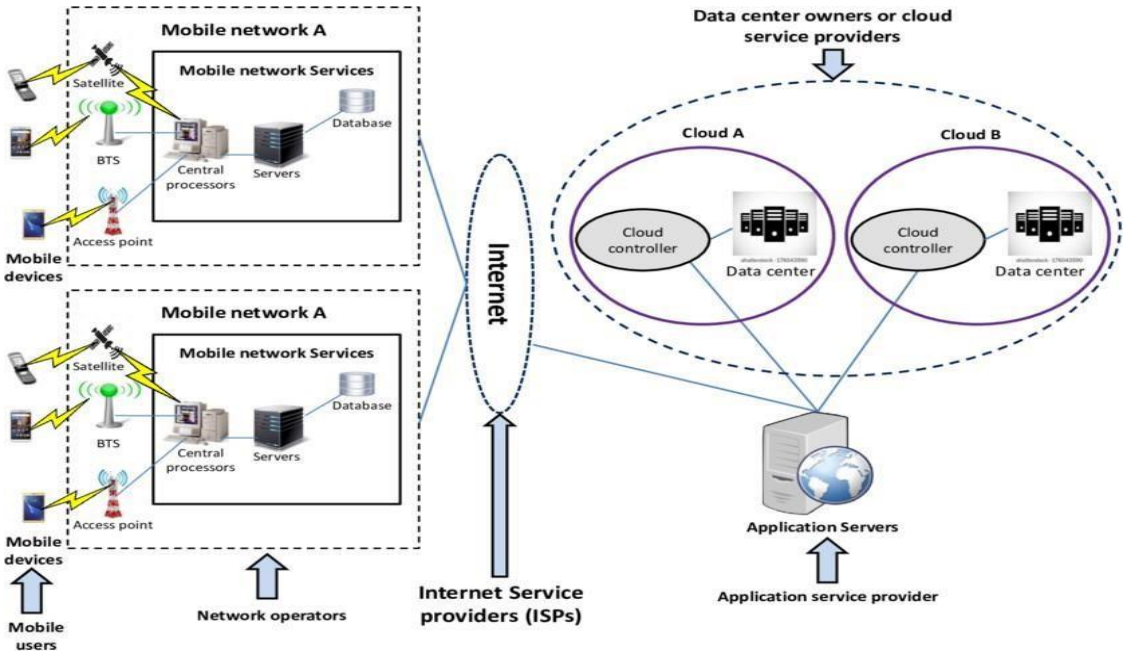


Figure 5. An architecture for distributed mobile cloud computing

10. CONCLUSION

A careful examination of the details and comparison graphs in Section 6 makes it evident that mobile cloud computing and distributed cloud computing both have unique advantages and applications. Lowering latency times, offering high processing capacities, effectively using cloud electricity, and reducing major processing power requirements have been the main goals of previous distributed cloud computing research projects. Even though researchers have made great strides in enhancing data processing streams and facilitating scalability, there is still a gap in achieving optimal performance and resource consumption. However, mobile cloud computing, which prioritizes parallel processing and enhanced system efficiency, has emerged as a brilliant example of innovation. These advancements have solved long-standing problems such as identity-based signature systems, decreasing communication and calculation times, saving a significant amount of computation under high loads, and enhancing scalability. This study focuses on the area of mobile cloud computing, which the integration of cloud is computing into a mobile environment to enable users to access resources whenever they need them. Security protocols that are intended to prevent unauthorized access to sensitive data and information kept in the cloud are the main issues with mobile cloud computing. As we outline our future research plans, security concerns must be carefully taken into account while developing mobile cloud solutions. By addressing these security issues head-on, we can build a more robust and resilient mobile cloud ecosystem that meets users' evolving needs while upholding the highest standards of data privacy and security.In essence, despite offering distinct advantages and areas of focus, distributed cloud computing and mobile cloud computing both demonstrate the transformative potential of cloud technology in revolutionizing the digital world. As we navigate the complexities of a world that is becoming more interconnected, it is crucial to take advantage of the synergies between dispersed and mobile cloud computing. Customers will have unparalleled access to computing resources as a result, and

cooperation and creativity will be encouraged. We can fully fulfill the potential of mobile cloud computing and usher in a new era of digital empowerment and excellence by utilizing thorough research and strategically placed investments in security and performance enhancement.

REFERENCES

1. Asghari, A., & Sohrabi, M. K. (2024). Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. Computer Science Review, 51, 100616.
2. Afek, Y., Giladi, G., & Patt-Shamir, B. (2024). Distributed computing with the cloud. Distributed Computing, 37(1), 1-18.
3. Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), 11-30.
4. Bi, C., Li, J., Feng, Q., Lin, C. C., & Su, W. C. (2024). Optimal deployment of vehicular cloud computing systems with remote microclouds. Wireless Networks, 30(6), 5305-5317.
5. Mir, A. A. (2024). Optimizing Mobile Cloud Computing Architectures for Real-Time Big Data Analytics in Healthcare Applications: Enhancing Patient Outcomes through Scalable and Efficient Processing Models. Integrated Journal of Science and Technology, 1(7).
6. Kanwal, A., Amjad, T., & Ashraf, H. (2024). Framework for Agent-Based Multistage Application Partitioning Algorithm in Mobile Cloud Computing. SN Computer Science, 5(4), 330.
7. Khalaf, O. I., Anand, D., Abdulsahib, G. M., & Chandra, G. R. (2024). Original Research Article A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems. Journal of Autonomous Intelligence, 7(3).
8. Khalaf, O. I., Anand, D., Abdulsahib, G. M., & Chandra, G. R. (2024). Original Research Article A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems. Journal of Autonomous Intelligence, 7(3).
9. Dhanasekaran, S., Rajput, K., Yuvaraj, N., Aeri, M., Shukla, R. P., & Singh, S. K. (2024, May). Utilizing Cloud Computing for Distributed Training of Deep Learning Models. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.
10. Pramanik, P. K. D., Pal, S., & Choudhury, P. (2024). Mobile crowd computing: potential, architecture, requirements, challenges, and applications. The Journal of Supercomputing, 80(2), 2223-2318.
11. William, D., & Bommu, R. (2024). Harnessing AI and Machine Learning in Cloud Computing for Enhanced Healthcare IT Solutions. Unique Endeavor in Business & Social Sciences, 3(1), 70-84.
12. Raghav, Y. Y., & Kait, R. (2024). Edge computing empowering distributed computing at the edge. In Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models (pp. 67-83). IGI Global.
13. Mahesar, A. R., Li, X., & Sajnani, D. K. (2024). Efficient microservices offloading for cost optimization in diverse MEC cloud networks. Journal of Big Data, 11(1), 123.
14. Anandappa, M., & Mudnal, M. K. (2024). Cloud computing and security issues in the cloud. Journal of Scientific Research and Technology, 59-66.
15. Rajagopalan, A., Swaminathan, D., Bajaj, M., Damaj, I., Rathore, R. S., Singh, A. R., ... & Prokop,
L. (2024). Empowering power distribution: Unleashing the synergy of IoT and cloud computing for sustainable and efficient energy systems. Results in Engineering, 101949.
16. Asghari, A., & Sohrabi, M. K. (2024). Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. Computer Science Review, 51, 100616.
17. Zeebaree, I. (2024). The Distributed Machine Learning in Cloud Computing and Web Technology: A Review of Scalability and Efficiency. Journal of Information Technology and Informatics, 3(1).
18. Yadav, S. K., & Kumar, R. (2024). ASME-SKYR framework: A comprehensive task scheduling framework for mobile cloud computing. Wireless Networks, 30(3), 1221-1244.
19. Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), 11-30.

20. Dhinakaran, D., Selvaraj, D., Dharini, N., Raja, S. E., & Priya, C. (2024). Towards a novel privacy- preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution. arXiv preprint arXiv:2407.18923.
21. Hassan, M. U., Al-Awady, A. A., Ali, A., Iqbal, M. M., Akram, M., & Jamil, H. (2024). Smart Resource Allocation in Mobile Cloud Next-Generation Network (NGN) Orchestration with Context-Aware Data and Machine Learning for the Cost Optimization of Microservice Applications. Sensors, 24(3), 865.
22. Khalaf, O. I., Anand, D., Abdulsahib, G. M., & Chandra, G. R. (2024). Original Research Article A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems. Journal of Autonomous Intelligence, 7(3).
23. Mondal, R. (2024). Mobile Cloud Computing. In Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models (pp. 170-185). IGI Global.
24. Alabdeli, H., Yamsani, N., Anitha, D., Chaithra, K. N., & Bindu, G. (2024, February). Intrusion Detection System in Mobile Cloud Computing Using Bat Optimization Algorithm-Support Vector Machine. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-4). IEEE.
25. Pramanik, P. K. D., Pal, S., & Choudhury, P. (2024). Mobile crowd computing: potential, architecture, requirements, challenges, and applications. The Journal of Supercomputing, 80(2), 2223-2318.
26. Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.
27. Fadhil, J., & Zeebaree, S. R. (2024). Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges. Indonesian Journal of Computer Science, 13(2).
28. Fadhil, J., & Zeebaree, S. R. (2024). Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges. Indonesian Journal of Computer Science, 13(2).
29. Anandappa, M., & Mudnal, M. K. (2024). Cloud computing and security issues in the cloud. Journal of Scientific Research and Technology, 59-66.
30. Taher, H., & Zeebaree, S. R. (2024). Harnessing the Power of Distributed Systems for Scalable Cloud Computing A Review of Advances and Challenges. Indonesian Journal of Computer Science, 13(2).
31. Khan, S., Jiangbin, Z., Irfan, M., Ullah, F., & Khan, S. (2024). An expert system for hybrid edge to cloud computational offloading in heterogeneous MEC–MCC environments. Journal of Network and Computer Applications, 225, 103867.
32. Verma, G. (2024). Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence, 36(1), 147-160.
33. Kumar, A., Boreda, D., & Vishwakarma, S. (2024, April). Redesigned Cloud Service Migration Techniques for Improved Portability. In 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 550-554). IEEE.
34. Soni, P. K., & Dhurwe, H. (2024). Challenges and Open Issues in Cloud Computing Services. In Advanced Computing Techniques for Optimization in Cloud (pp. 19-37). Chapman and Hall/CRC.
35. Murad, S. A., Azmi, Z. R. M., Muzahid, A. J. M., Sarker, M. M. H., Miah, M. S. U., Bhuiyan, M.
K. B., ... & Bairagi, A. K. (2024). Priority based job scheduling technique that utilizes gaps to increase the efficiency of job distribution in cloud computing. Sustainable Computing: Informatics and Systems, 41, 100942.
36. Merseedi, K. J., & Zeebaree, S. R. (2024). The cloud architectures for distributed multi-cloud computing: a review of hybrid and federated cloud environment. Indonesian Journal of Computer Science, 13(2).
37. Jiang, Q., Xu, X., Bilal, M., Crowcroft, J., Liu, Q., Dou, W., & Jiang, J. (2024). Potential game based distributed IoV service offloading with graph attention networks in mobile edge computing. IEEE Transactions on Intelligent Transportation Systems.
38. Sinha, A., Banerjee, P., Roy, S., Rathore, N., Singh, N. P., Uddin, M., ... & Alsaqour, R. (2024). Improved Dynamic Johnson Sequencing Algorithm (DJS) in Cloud Computing Environment for
Efficient Resource Scheduling for Distributed Overloading. Journal of Systems Science and Systems Engineering, 1-34.
39. Wang, Y., Yang, C., Lan, S., Zhu, L., & Zhang, Y. (2024). End-edge-cloud collaborative computing for deep learning: A comprehensive survey. IEEE Communications Surveys & Tutorials.
40. Kaur, S. (2024). Novel Encryption Technique for Cloud Computing Access Control. In Advancing Sustainable Science and Technology for a Resilient Future (pp. 323-326). CRC Press.
41. Gupta, M., & Singla, N. (2019). Evolution of cloud in big data with hadoop on docker platform. In *Web services: Concepts, methodologies, tools, and applications* (pp. 1601-1622). IGI Global.

42. Gupta, M., Yadav, R., & Tanwar, G. (2016, March). Insider and flooding attack in cloud: A discussion. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 530-535). IEEE.
43. Sharma, H., Kumar, R., & Gupta, M. (2023, March). A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network. In *2023 2nd International Conference for Innovation in Technology (INOCON)* (pp. 1-5). IEEE.
44. Kumar, P., Gupta, M., & Kumar, R. (2023, July). Improved cloud storage system using ipfs for decentralised data storage. In *2023 International Conference on Data Science and Network Security (ICDSNS)* (pp. 01-06). IEEE.
45. Gupta, M., Kumar, R., Kumar, A., & Chaurasia, P. (2023, December). Virtual Board based Data Sharing Application Using Cloud Computing. In *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1494-1498). IEEE.
46. Gupta, M., Kumar, R., Maheshwari, M., & Kumar, R. (2023, December). Drones and Networks: Ensuring safe and secure operations using 5g mobile network. In *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1239-1242). IEEE.

AI-Driven Intrusion Detection System

Jaya Venkatesh Thirumalasetti, Akshi Jain, Kartik Bansal, Kartik Bansal, Ashbi Biju

Department of CSE, Apex Institute of Technology, Chandigarh University, Punjab, India
jayavenkatesh2004@gmail.com, jain.akshigr@gmail.com, kartikbansal1911@gmail.com, ashbibiju5@gmail.com

ABSTRACT

An Intrusion detection system (IDS) helps safeguard computer networks against malicious attacks and abnormal activity. It faces challenges with false positive, and false negatives and their susceptibility to evasion attacks. This research paper focuses on augmenting IDS with the power of Convolutional Neural Networks (CNN) and Random Forest, algorithms in machine learning for attack classification. The first part of the study delves into categorizing attacks into different categories including signature-based attacks, anomalybased attacks, and hybrid attacks. This classification helps in understanding the attack landscape and tailoring effective solutions. The second part outlines an approach, combining the robustness of CNN and the classification prowess of Random Forest to improve the accuracy of intrusion detection. Both algorithms are used for classifying tasks, CNN is a powerful tool of deep learning that helps in enhancing the accuracy of IDS detection by identifying/classifying attacks based on the learned features as it is capable of automatically learning patterns and anomalies whereas Random Forest provides a more refined classification of the attacks. This study demonstrates that the fusion of CNN and Random Forest in machine learning significantly enhances the detection of known attacks, making IDS more resilient and adaptable. It presents a comprehensive solution to intrusion detection challenges, promoting computer network security in the face of evolving cyber threats.

Keywords: *Intrusion detection, Machine Learning, Cost Matrix*

1. INTRODUCTION

Today, computer networks are the lifeblood of modern society, enabling communication, commerce, and the exchange of vital information all over the world. This connectivity comes with the looming threat of malicious attacks, cyber threats, online privacy threats and many more that can potentially cripple, compromise or steal valuable insights from these networks. In an interconnected world, protecting individual nodes from threats and vulnerabilities is not enough; the network as a whole needs to be secured. Businesses and organizations face a variety of security risks, such as denial-of-service attacks, phishing schemes that are getting more and more sophisticated, and illegal access to data [1]. The operation of the entire network can be jeopardized by a single point of failure or successful intrusion, with disastrous results such as data leaks, monetary losses, and a decline in customer trust [2]. Businesses and organizations now face a variety of risks, such as ransomware, distributed denial of service (DDoS) attacks, unauthorized data access, and increasingly clever phishing schemes, in addition to the simple, easily identifiable threats of the past [3]. However, these systems face significant challenges including false positives and false negatives as well as the constant evolution of evasion attacks that seek to bypass their defenses.

This search's foundation lies in the classification of 3 types of attacks including signaturebased, anomaly- based and hybrid attacks [4]. This categorization provides a better understanding of the attacks and allows for tailored and effective solutions to the problem. Signature-based attacks are well-known patterns of intrusion, whereas anomaly-based attacks involve deviations

from normal network behavior. Hybrid attacks, as the name suggests, combine elements of both [5]. The core focus of this paper is on the innovative approach that harnesses the combined power of Convolutional Neural Network (CNN) and Random Forest in the realm of machine learning [6]. Both algorithms are used for classifying tasks, CNN is a powerful tool of deep learning that helps in enhancing the accuracy of IDS detection by identifying/classifying attacks based on the learned features as it is capable of automatically learning patterns and anomalies whereas Random Forest provides a more refined classification of the attacks [7].

Random Forest is capable of handling non-linear data and can distinguish between various classes of networks. By integrating Random Forest into the classification process, this research ensures that the IDS can identify different types of threats easily [8]. In summary, this research paper contributes to the field of intrusion detection by offering a comprehensive solution that augments the accuracy, recognizing different types of attacks, and adaptability of IDS in the face of evolving cyber threats [9]. The fusion of CNNs and SVMs in machine learning provides a powerful tool for the detection of known attacks, significantly improving the security posture of computer networks [10]. As the digital landscape continues to evolve, these research findings promise to provide a robust defense mechanism that safeguards networks against a multitude of threats, ultimately enhancing the overall security and trustworthiness of our interconnected world.

2. LITERATURE SURVEY

Our project seeks to create an SVM and CNN-based intrusion detection system (IDS) to identify and recognize real-time threats, anomalies and malicious activities. In recent years the detection and identification of attacks have become more automated and diverse with the help of machine learning and deep learning algorithms. Stefan Axelsson et al. discussed a need for an up to date intrusion detection system. The authors discussed about HyperView [DBS92] system and its 2 components [11]. The ordinary expert system which checks the trails for an incoming attack. Neural network-based component which tries to understand the behaviour of a user and raises an alarm if any suspicious activity is found. Ansam Khraisat et al. [12] warned about the alarmingly increasing sophistication level for cyber criminals. They classified the cyber-attacks into two different categories i.e., Signature-based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). The authors also discussed problem of maintaining the information about new types of attacks especially which yield high false alarms and result in poor accuracy. The authors also suggested several evasion techniques by attackers to avoid detection.

Faiza Medjek's research paper [13] described the initial stages of developing, a new Intrusion Detection System using Machine Learning (ML) to detect routing attacks against RPL. They recorded detection rate (Recall), precision, and F1-score for multi-class classification which was more than 98% for the three classifiers, while the KNN accuracy was 99%. Besides, Random Forest recorded the lowest fitting time.

Daniel L. Marino et al. [14] discussed about Adversarial machine learning approach to provide explanations for incorrect classifications made by traditional intrusion detection systems. The authors also visualized the most relevant features which explained the reason for the misclassification. Data imbalance is imperative due to its potential to result in a high rate of undetected network threats [15]. Recent research proposes a novel AI-based NIDS which leverages generative models to create synthetic data, also mitigating data imbalance and

demonstrating improved performance. This approach holds promise for enhancing network security in the face of evolving threats.

A taxonomy for the latest intrusion detection system methodologies, approaches and technologies was proposed by Hung-Jen Liao [16]. Here the authors described the supremacy and limitations which should be considered while selection an approach.

Adnan Mohsin Abdulazeez et al. [17] proposed on a taxonomy of IDS, which uses the primary dimension of data objects to classify and sum up IDS literatures based on and dependent on deep learning. They assumed the kind of taxonomy which is sufficient for researchers in cyber security. The random forest classifier outperforms better with accuracy of 99.98% based on the results.

Taeshik Shon who was focused on machine learning techniques for detecting attacks from internet anomalies [18]. By experiment they also demonstrated that their proposed framework outperforms currently employed real-world MDS. The overall goal of Enhanced SVM approach was to provide a general framework for detection and classification of novel attacks in network traffic.

R. Vinayakumar et al. [19] worked on a deep neural network (DNN), a type of deep learning model, which is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyberattacks.They proposed a hybrid intrusion detection alert system using a highly scalable framework on commodity hardware server which has the capability to analyze the network and host-level activities. Their framework employed distributed deep learning model with DNNs for handling and analyzing very large-scale data in real-time.

Zeeshan Ahmad [20] in his article, clarified the concept of IDS and then provided the taxonomy based on the notable ML and DL techniques adopted in designing network-based IDS (NIDS) systems. A comprehensive review of the recent NIDS-based articles is provided by discussing the strengths and limitations of the proposed solutions. Then, recent trends and advancements of ML and DL-based NIDS are provided in terms of the proposed methodology, evaluation metrics, and dataset selection.

Monali Shetty et al. [21] presented an overview of real time data mining-based intrusion detection system (IDSs). They focused on issues related to deploying a data mining -based IDS in a real time environment. New intelligent Intrusion Detection Systems (IDSs) are based on sophisticated algorithms rather than current signature-base detections are in demand. They proposed a new real time data-mining based technique for intrusion detection using an ensemble of binary classifiers with feature selection and multi boosting simultaneously.

Jabez J et al. [22] proposed a new approach called outlier detection where, the anomaly dataset is measured by the Neighborhood Outlier Factor (NOF). Here, trained model consists of big datasets with distributed storage environment for improving the performance of Intrusion Detection system. The training model consists of big datasets with distributed environment that improves the performance of Intrusion detection system. The proposed approach has also been tested with the KDD datasets that were received from real world. The machine learning approaches detect the intrusion in the computer network with huge execution time and storage

to predict when compared to the proposed IDS system which takes less execution time and storage to test the dataset.

Kingsly Leung [23] presented a new density-based and grid- based clustering algorithm that is suitable for unsupervised anomaly detection. They evaluated a new approach in unsupervised anomaly detection in the application of network intrusion detection. The new approach, fpMAFIA, is a density-based and grid-based high dimensional clustering algorithm for large data sets.

Iqbal H. Sarker [24] presented an Intrusion Detection Tree ("IntruDTree") machine-learningbased security model that first takes into account the ranking of security features according to their importance and then build a tree-based generalized intrusion detection model based on the selected important features. This model is not only effective in terms of prediction accuracy for unseen test cases but also minimizes the computational complexity of the model by reducing the feature dimensions.

Hamed Alqahtani et al. [25] employed various popular machine learning classification algorithms, namely Bayesian Network, Naive Bayes classifier, Decision Tree, Random Decision Forest, Random Tree, Decision Table, and Artificial Neural Network, to detect intrusions due to provide intelligent services in the domain of cyber-security.

3. METHODOLOGY A. Data Collection

Domain	Overview
IPV4_SRC_ADDR	The IPv4 source address that serves as the origin of network traffic.
L4_SRC_PORT	Communication's source port number at the transport layer, which is often TCP or UDP.
IPV4_DST_ADDR	IPv4 address used as the destination where network traffic is routed.
L4_DST_PORT	The service or application that the traffic is meant for is indicated by the destination port number at the transport layer.
PROTOCOL	ICMP, TCP, UDP, or any other network layer protocol in use.
L7_PROTO	The particular application-level protocol being used, such as HTTP, FTP, or DNS, is referred to as the Layer 7 protocol.
IN_BYTES	The amount of data received in this network flow in bytes.
OUT_BYTES	The total bytes transmitted during this network flow.

IN_PKTS	The number of packets that have arrived in this flow.

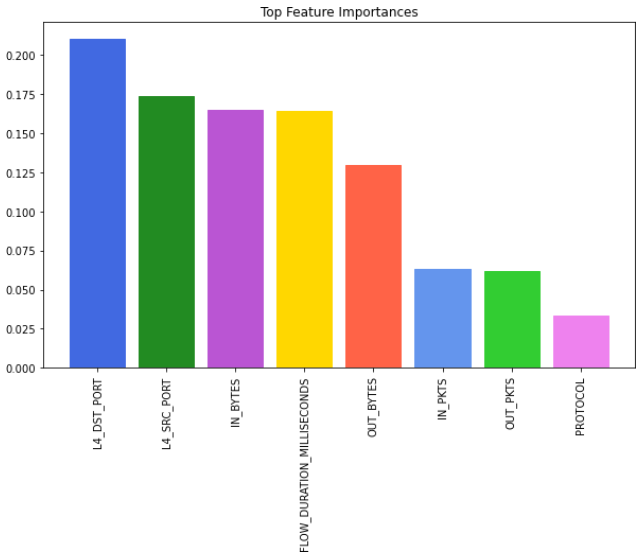
The NF-UQ-NIDS dataset is an extensive collection of network flow data that was used in this study. It includes a wide variety of network configurations and attack scenarios, offering a sizable dataset for the creation and assessment of intrusion detection systems. There are 11,994,893 entries in the NF-UQ-NIDS dataset overall. Of those, 9,208,048 (76.77%) show benign network flows, whereas 2,786,845 (23.23%) show different kinds of network attacks. We were able to take advantage of shared feature sets by merging several smaller datasets to form the NF-UQ-NIDS dataset. A more comprehensive and universal dataset was produced by integrating multiple sources of network flow data.

B. Data Preprocessing:

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

C. Feature Selection:

A key component of our approach was feature selection. We gave great thought to the features to incorporate into our models in order to improve the intrusion detection system's performance. In order to maximize the model's efficiency, this stage comprised deleting aspects that were unnecessary or redundant.



D. Model Training:

Convolutional Neural Networks (CNN) and Random Forest are the two unique models that we have chosen. Random Forest and CNN are two models that were selected due to their ability to handle tabular data that combines numerical and categorical features, and their complementary strengths in capturing complex patterns in network traffic data. **E. Columns in dataset:**

OUT_PKTS	The number of packets that are being sent out in this flow.
TCP_FLAGS	TCP-specific flags, such as SYN, ACK, FIN, or other control flags.
FLOW_DURATION_MILLISECONDS	The length of time the network flow was active, measured in milliseconds.
Label	Network flow labeling, which could reveal if the flow is regarded as normal or suspicious.
Attack	A particular kind of attack found in the flow

F. Random Forest:

An ensemble of decision trees was used to set up the Random Forest model, and performance was optimized by adjusting hyperparameters like tree depth and the number of estimators.

G. Testing and Evaluation:

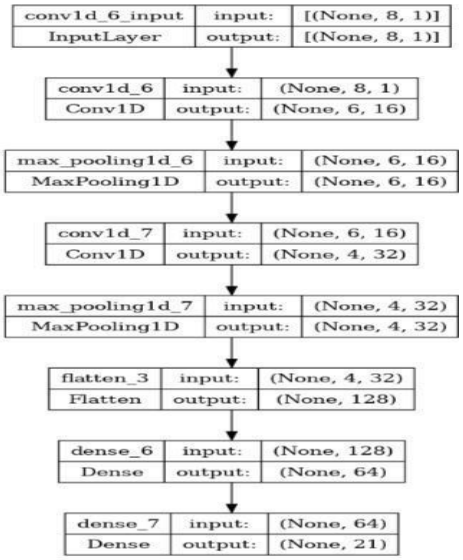
We will use accuracy as the main metric to assess the models' performance once they have been trained. To solve our research problem, we want to determine which model, or models, will be the most accurate.

H. CNN:

Multiple convolutional and pooling layers preceded fully connected layers in the CNN architecture. Activation functions, number of filters, and kernel size were among the hyperparameters that we adjusted to maximize the model's capacity to extract pertinent features from network flow data.

4. RESULT AND ANALYSIS

In this paper, we investigated the performance of two different machine learning models for the Intrusion Detection System (IDS) task in a network environment: Random Forest and Convolutional Neural Networks (CNN). We assessed these models' performance using a range of metrics, paying close attention to accuracy since it is so important in the context of intrusion detection system (IDS).

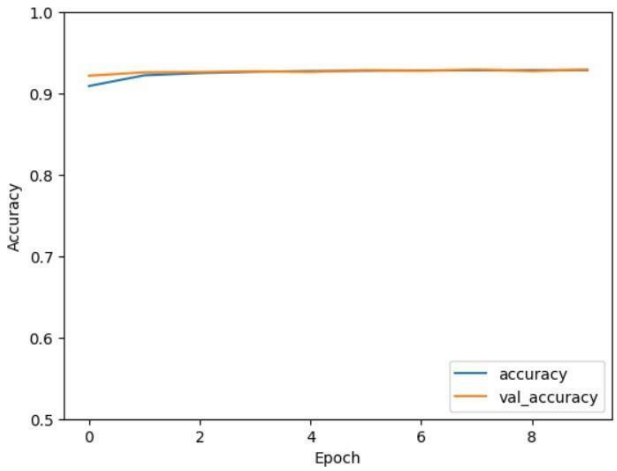


The main performance metric employed in this study was accuracy, which assesses how well the models were able to categorize network traffic as either benign or malevolent. To learn more about the models' abilities to discern between true positives, false positives, true negatives, and false negatives, we also looked at precision, recall, and F1-score.

The results of our experiments revealed the following performance metrics for the CNN and Random Forest models:

A. CNN:

Accuracy: 92.94%



B. Random Forest Model:

Accuracy: 92%
Precision : 0.91
Recall: 0.92
F1-score: 0.91

5. Conclusion

In this study, we carried out a thorough analysis of the effectiveness of Random Forest and Convolutional Neural Networks (CNN) models for the Intrusion Detection System (IDS) task in a network environment. By analyzing these models' accuracy, precision, recall, and F1score

in identifying malicious or legitimate network traffic, we were able to determine how effective they were. According to our findings, the CNN and Random Forest models are both quite good at identifying network intrusions, though the CNN model does so with a marginally higher accuracy rate than the RF model. Both models demonstrate promising high accuracy rates, indicating their potential for practical network security applications. It is important to weigh several factors, including interpretability, scalability, and computational complexity, when deciding between the CNN and Random Forest models. Even though the CNN model proved to be more accurate, the RF model is still a competitive option with its own benefits.

REFERENCES

[1] P. Kumar, M. Gupta and R. Kumar, "Improved Cloud Storage System Using IPFS for Decentralised Data Storage," 2023 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2023, pp. 01-06, doi: 10.1109/ICDSNS58469.2023.10245317.

[2] Gupta, M., Chaudhary, G., Bansal, D., & Pandey, S. (2022). DTLMV2—A real-time deep transfer learning mask classifier for overcrowded spaces. Applied Soft Computing, 127, 109313.

[3] Kumar, S., Kumar, R., Gupta, M., & Obaid, A. J. (2024, January). Deep Learning-Based Web Application for Real-Time Apple Leaf Disease Detection and Classification. In 2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-6). IEEE.

[4] Gupta, M., Gupta, A., & Arora, S. (2022). Addressing the security, privacy, and trust issues in IoTenabled CPS. In Handbook of Research of Internet of Things and Cyber-Physical Systems (pp. 433-452). Apple Academic Press.

[5] Gupta, A., Kumar, R., & Kumar, Y. (2023). An automatic speech recognition system in Indian and foreign languages: A state-of-the-art review analysis. Intelligent Decision Technologies, 17(2), 505-526.

[6] Goyal, B., Pandey, A. K., Kumar, R., & Gupta, M. (2023, July). Disease detection in potato leaves using an efficient deep learning model. In 2023 International Conference on Data Science and Network Security (ICDSNS) (pp. 01-05). IEEE.

[7] Gupta, M., Ved, C., & Kumari, M. (2022). Emergence of Blockchain Applications with the 6G-Enabled IoT-Based Smart City. In Blockchain for 6G-Enabled Network-Based Applications (pp. 213235). CRC Press.

[8] Dewari, S., Gupta, M., Kumar, R., Obaid, A. J., & AL-Hameed, M. R. (2023). A review analysis on measuring the soil characteristic in agriculture using artificial intelligence and IOT. In Micro-Electronics and Telecommunication Engineering: Proceedings of 6th ICMETE 2022 (pp. 325-334). Singapore: Springer Nature Singapore.

[9] Sharma, P., Kumar, R., & Gupta, M. (2023, May). Road features extraction using convolutional neural network. In 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT) (pp. 881-886). IEEE.

[10] Baruah, A., Kumar, R., & Gupta, M. (2023, May). Traffic sign recognition using deep learning neural network and spatial transformer. In 2023 international conference on advances in computing, communication and applied informatics (ACCAI) (pp. 1-8). IEEE.

[11] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy.

[12] https://www.sciencedirect.com/science/article/abs/pii/S187454822100 0287

[13] Medjek, F., Tandjaoui, D., Djedjig, N., & Romdhani, I. (2021). Fault-tolerant AI-driven intrusion detection system for the internet of things. *International Journal of Critical Infrastructure Protection*, *34*, 100436.

[14] Marino, D. L., Wickramasinghe, C. S., & Manic, M. (2018, October). An adversarial approach for explainable ai in intrusion detection systems. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society* (pp. 3237-3243). IEEE.

[15] Park, C., Lee, J., Kim, Y., Park, J. G., Kim, H., & Hong, D. (2022). An enhanced AI-based network intrusion detection system using generative adversarial networks. *IEEE Internet of Things Journal*, *10*(3), 2330-2345.

[16] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of network and computer applications, 36(1), 16-24.

[17] Amanoul, S. V., Abdulazeez, A. M., Zeebare, D. Q., & Ahmed, F. Y. (2021, June). Intrusion detection systems based on machine learning algorithms. In *2021 IEEE international conference on automatic control & intelligent systems (I2CACIS)* (pp. 282-287). IEEE.

[18] Shon, T., Kim, Y., Lee, C., & Moon, J. (2005, June). A machine learning framework for network anomaly detection using SVM and GA. In *Proceedings from the sixth annual IEEE SMC information assurance workshop* (pp. 176-183). IEEE.

[19] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE access*, *7*, 41525-41550.

[20] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150.

[21] https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c427ed27272cb98c29eaef520a7a982e7ab7a184

[22] Jabez, J., & Muthukumar, B. J. P. C. S. (2015). Intrusion Detection System (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science*, *48*, 338-346.

[23] Leung, K., & Leckie, C. (2005, January). Unsupervised anomaly detection in network intrusion detection using clusters. In *Proceedings of the Twenty-eighth Australasian conference on Computer ScienceVolume 38* (pp. 333-342).

[24] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 754.

[25] Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore.

Using Chatgpt's Ai-Powered Language Processing Technology In Software Development: A Test Module Example

Zöhre Serttaş[1] , Fadi Al-Turjman[1]

[1] *Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey* *zohre.serttas@neu.edu.tr*

[1] *Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey* *fadi.alturjman@neu.edu.tr*

ABSTRACT

AI powered technologies have brought significant transformation to software development processes, as in many other fields in recent years. ChatGPT, developed by OpenAI, is a language model with natural language processing capabilities that supports software developers in various areas such as code generation, debugging, and optimization. In this study, the use of ChatGPT in software development processes was tested through a module. For the test, ChatGPT 4.0 was asked to write a "Data Analysis Module for a Mobile Digital Forensics Application" using Python. The command details of the module are explained in detail in the methodology section of the study. The study evaluates the effectiveness of ChatGPT through theoretical analyses and practical examples, aiming to reveal the strengths and weaknesses of the model. It examines how ChatGPT can generate code in various programming languages, evaluates the performance of these codes, and explores the model's role in debugging processes. The study highlights the model's strengths, particularly in areas such as fundamental algorithms, data processing, bug fixing, and code optimization. However, it also notes that the model carries the risk of occasionally producing incorrect or incomplete code in complex or ambiguous inputs. As a result, the study presents findings obtained through practical examples and testing of these codes. It also concludes that while ChatGPT is a valuable assistant tool in software development processes, it must be supported by human supervision and testing. This study provides theoretical analyses and practical examples to understand the effectiveness and limitations of ChatGPT, offering insights for future research.

Keywords: Language Processing, ChatGPT, Python, Mobile Forensics

1. INTRODUCTION

Artificial intelligence is used in many fields such as problem-solving, game modeling, information processing, automated theorem proving, expert systems, natural language processing, speech analysis, pattern recognition, computer-aided creativity, and robotics (Nabiyev & Erümit, 2022). One of these fields, natural language processing (NLP), is an important area of study that combines artificial intelligence with linguistics (Fanni, Febi, Aghakhanyan & Neri, 2023). NLP is effectively utilized in various applications, including spelling correction, digitization of printed texts, text summarization and interpretation, access to information within content, writing suggestions, foreign language translations, the development of language-supported reading and writing tools, and more (Kang, Cai, Tan, Huang & Liu, 2020). These processes involve analyzing word groups, recognizing grammatical rules, and understanding the structural elements of language. The ultimate goal is to make human language comprehensible and processable by machines.

Today the capabilities of natural language processing enable the development of spellcheck suggestions, auto-correction systems, voice assistants, interactive voice response systems used by banks and other institutions, online translation tools, text-to-speech applications, and software that converts voice recordings into text. Additionally, various AIpowered tools can communicate meaningfully with humans through written or spoken interactions using NLP capabilities. Advances in NLP have also contributed to the emergence of new ideas for the educational use of artificial intelligence. Software programs that automate business processes and operate under computer control are generally referred to as “bots” (Völker & Weske, 2021). The history of chatbots, which enhance the communication capabilities of devices and generate automated responses, dates back to the 1960s (Kuruca, Üstüner & Şimşek, 2022). Over time, these bots have evolved with AI support, allowing them not only to generate simple responses but also to understand users and provide more complex and meaningful answers. Chatbots are now actively used in many fields, particularly in voice response systems (İşeri, Aydin & Tutuk, 2021).

One of the most advanced chatbots, ChatGPT, is capable of understanding users' written input in various languages and generating meaningful responses. ChatGPT is powered by AI, enabling it to provide coherent answers to user queries through advanced machine learning (Karakoç Keskin, 2023). Its usability in education is noteworthy, as it facilitates access to information for students and supports interactive learning processes. Advances in AI technologies have significantly contributed to individual learning processes. In particular, generative AI tools have begun to offer various applications in the education sector. One of the most prominent examples is the generation of code blocks and software. ChatGPT is capable of teaching programming languages. While a traditional instructor may specialize in a few programming languages, ChatGPT provides knowledge in many languages, including Python, Java, JavaScript, C++, C#, Ruby, Swift, Go, PHP, TypeScript, Kotlin, and Rust (Idrisov & Schlippe, 2024). Additionally, it simplifies transitions between different programming languages by enabling code conversion and adaptation. This capability offers a significant advantage in coding education. A detailed explanation of this process is provided in Figure 1.

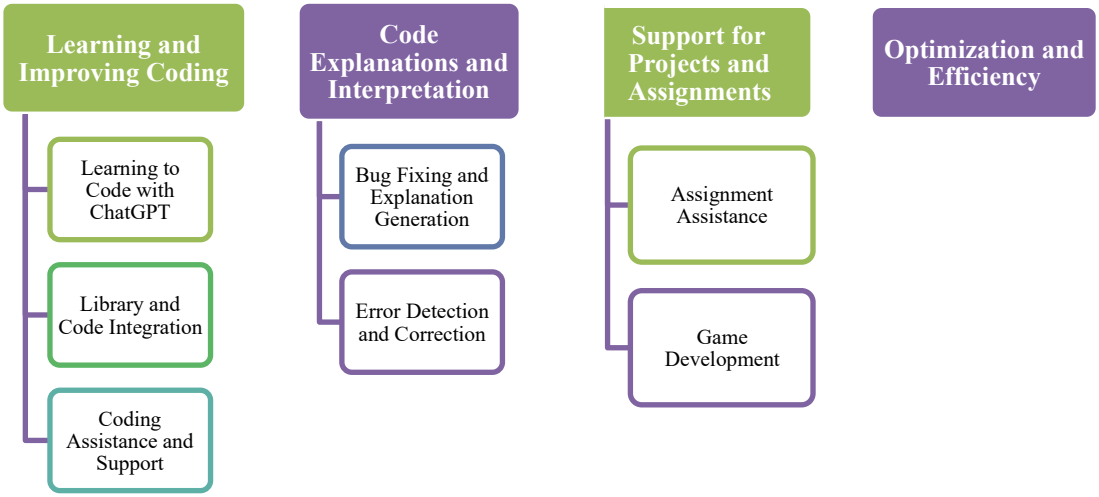


Figure 1. Current Use Cases of ChatGPT in Coding Processes

In light of all this information, a test module example was used to examine how ChatGPT generated code blocks can be utilized in the software development process. The situations encountered during the study process have been shared, and the entire procedure has been detailed in the methodology section.

2. METHOD

This study is an applied research that examines the applicability of a test module example to explore how ChatGPT's code blocks can be utilized in the software development process. An experimental approach was adopted during the study, and the test module development and integration processes were implemented step by step for analysis. Application-based analyses and comparative evaluations were used in the study. The areas of use are explained in detail in Table 1.

Table 1. *Testing Processes*

Test Name	Test Description	Test Result
Code Development and Implementation	ChatGPT generated code was used to create a test module.	+
Functional Tests	Test scenarios were applied to examine the functionality and accuracy of the code.	+
Code Comparison	ChatGPT generated code was compared with manually written code in terms of error rate, efficiency, and readability.	+
Performance Analysis	The impact of the code on error rate, efficiency, and the integration process was analyzed.	+

2.1. Application Process

Table 2. *Code Generation and Integration Testing with ChatGPT*

Test Name	Test Description	Test Result
Code Generation with ChatGPT	Codes suitable for the test module have been created.	+
Code Integration	The obtained codes are integrated into the specified software project.	+

Code generation and integration testing with chatGPT In this test, code generation and integration with ChatGPT were evaluated, and it was confirmed that the generated code was suitable for the test module Table 2. The generated code was successfully integrated into the software project.

Application of Tests:

Table 3. *Unit, Result Analysis for Integration Tests*

Test Name	Test Description	Test Result
Unit Tests	It was implemented to measure the correctness of the code in independent units.	+
Integration Tests	It was examined whether the generated code worked in harmony with other components.	+
Analysis of Results	The codes were evaluated based on criteria such as accuracy, error rate, runtime and readability.	+

2.2. Code Block Generation and Testing

This section covers how ChatGPT 4.0 generates code based on a specific command and the process of evaluating its accuracy.

Command: Data Analysis Module for a Mobile Digital Forensics Application

ChatGPT 4.0 was given a command prompt to generate a module that analyzes data retrieved from a device for integration into a mobile application used in digital forensics.

User Prompt:
Write a Python module for a mobile application used in digital forensics that analyzes data retrieved from a device and reports suspicious activities.

Code Blocks;

```python
import json
from datetime import datetime

class ForensicAnalyzer:
    def __init__(self):
        self.suspicious_activities = []

    def load_device_data(self, file_path):
        """
        Cihazdan alınan verileri JSON formatında yükler.
        """
        try:
            with open(file_path, 'r') as file:
                data = json.load(file)
            return data
        except Exception as e:
            raise Exception(f"Veri yüklenirken hata oluştu: {e}")
```

```python
def analyze_data(self, data):
    """
    Cihaz verilerini analiz eder ve şüpheli aktiviteleri belirler.
    """
    try:
        for entry in data:
            timestamp = datetime.strptime(entry['timestamp'], '%Y-%m-%d %H:%M:%S')
            activity_type = entry.get('activity_type', '').lower()
            details = entry.get('details', '')

            # Şüpheli aktiviteleri belirleme kriterleri
            if activity_type == 'unauthorized_access':
                self.suspicious_activities.append({
                    "timestamp": timestamp,
                    "activity_type": activity_type,
                    "details": details
                })
```

```python
    elif 'suspicious' in details.lower():
        self.suspicious_activities.append({
            "timestamp": timestamp,
            "activity_type": activity_type,
            "details": details
        })

    except Exception as e:
        raise Exception(f"Veri analizi sırasında hata oluştu: {e}")
```

```python
def generate_report(self, output_path):
    """
    Şüpheli aktiviteleri JSON formatında bir rapora kaydeder.
    """
    try:
        report = {
            "generated_at": datetime.now().strftime('%Y-%m-%d %H:%M:%S'),
            "suspicious_activities": self.suspicious_activities
        }
        with open(output_path, 'w') as file:
            json.dump(report, file, indent=4, default=str)
        return f"Rapor başarıyla oluşturuldu: {output_path}"
    except Exception as e:
        raise Exception(f"Rapor oluşturulamadı: {e}")
```

```python
# Örnek Kullanım
if __name__ == "__main__":
    analyzer = ForensicAnalyzer()
    input_file = "device_data.json"  # Cihazdan alınan verilerin JSON dosyası
    report_file = "suspicious_activities_report.json"  # Raporun kaydedileceği dosya

    try:
        device_data = analyzer.load_device_data(input_file)
        analyzer.analyze_data(device_data)
        result = analyzer.generate_report(report_file)
        print(result)
    except Exception as e:
        print(e)
```

Figure 2. Code Block (1 Page)

Module Functions (load_device_data):

- Loads device data in JSON format.
- Returns an error message for data loading failures. **analyze_data:** - Identifies suspicious activities.

Example criteria:

Unauthorized_access:

- Details of suspicious behavior.

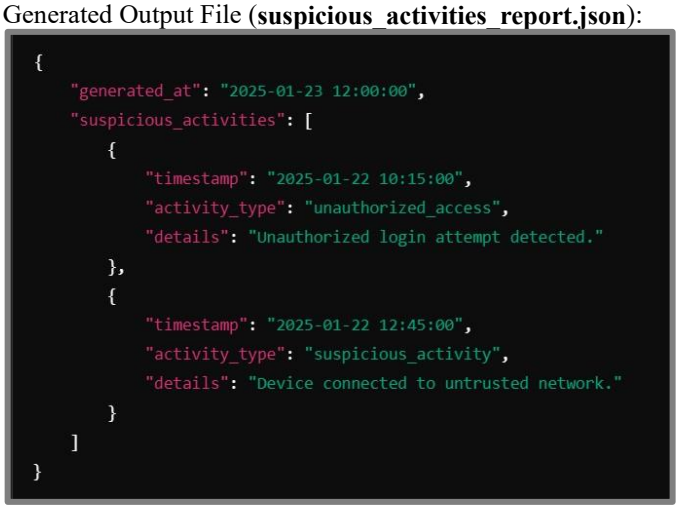
generate_report:

- Creates a report of suspicious activities.
- Saves it as a JSON file.

```
[
    {
        "timestamp": "2025-01-22 10:15:00",
        "activity_type": "unauthorized_access",
        "details": "Unauthorized login attempt detected."
    },
    {
        "timestamp": "2025-01-22 11:20:00",
        "activity_type": "normal_activity",
        "details": "User accessed normal application functionality."
    },
    {
        "timestamp": "2025-01-22 12:45:00",
        "activity_type": "suspicious_activity",
        "details": "Device connected to untrusted network."
    }
]
```


Figure 3. Sample Data (device_data.json)

Generated Output File (**suspicious_activities_report.json**):



```
{
    "generated_at": "2025-01-23 12:00:00",
    "suspicious_activities": [
        {
            "timestamp": "2025-01-22 10:15:00",
            "activity_type": "unauthorized_access",
            "details": "Unauthorized login attempt detected."
        },
        {
            "timestamp": "2025-01-22 12:45:00",
            "activity_type": "suspicious_activity",
            "details": "Device connected to untrusted network."
        }
    ]
}
```


Figure 5. Code Output

Kod çaliştirildiğinda konsola yazilan çikti;

```
Rapor başarıyla oluşturuldu: suspicious_activities_report.json
```


Figure 4. Code Output

2.3. Verification with Test Scenario

In this section of the study, a test scenario was created to verify the correct functioning of the written Python module, and the verification process was explained in detail.

Test Scenario:

Scenario Name: Identifying Suspicious Activities **Input:**

```
[
    {
        "timestamp": "2025-01-22 10:15:00",
        "activity_type": "unauthorized_access",
        "details": "Unauthorized login attempt detected."
    },
    {
        "timestamp": "2025-01-22 11:20:00",
        "activity_type": "normal_activity",
        "details": "User accessed normal application functionality."
    },
    {
        "timestamp": "2025-01-22 12:45:00",
        "activity_type": "suspicious_activity",
        "details": "Device connected to untrusted network."
    }
]
```


Figure 6. Test Scenario Input Screen

Expected Output:

- Suspicious activities should include records of type **unauthorized_access** and **suspicious_activity**. - The output JSON file (**suspicious_activities_report.json**) should be as shown in **Figure 7**.

```
{
    "generated_at": "2025-01-23 12:00:00",
    "suspicious_activities": [
        {
            "timestamp": "2025-01-22 10:15:00",
            "activity_type": "unauthorized_access",
            "details": "Unauthorized login attempt detected."
        },
        {
            "timestamp": "2025-01-22 12:45:00",
            "activity_type": "suspicious_activity",
            "details": "Device connected to untrusted network."
        }
    ]
}
```


Figure 7. Test Scenario Output Screen

Console Output:

```
Rapor başarıyla oluşturuldu: suspicious_activities_report.json
```


Figure 8. Test Scenario Console Output Screen

Test Results:

```
Rapor başarıyla oluşturuldu: suspicious_activities_report.json
```


Figure 9. Test Result Screen

```
{
    "generated_at": "2025-01-23 12:00:00",
    "suspicious_activities": [
        {
            "timestamp": "2025-01-22 10:15:00",
            "activity_type": "unauthorized_access",
            "details": "Unauthorized login attempt detected."
        },
        {
            "timestamp": "2025-01-22 12:45:00",
            "activity_type": "suspicious_activity",
            "details": "Device connected to untrusted network."
        }
    ]
}
```


Figure 10. Generated Code Block Output Screen

Test Result: - The program has correctly identified the specified suspicious activities.

- The JSON report was generated in the correct format with the expected content.
- The console output displayed the correct message.
- The program was successfully validated according to the given scenario.

3. CONCLUSION AND DISCUSSION

The data obtained in the research was evaluated using an application-based analysis method. During the research process:

- The functional accuracy and error rate of the code were analyzed.
- Code performance was examined in terms of processing time and efficiency.
- Developer feedback was taken into account to assess the readability and applicability of the code generated by ChatGPT.

Based on these methods, the contributions of ChatGPT to software development processes and its effectiveness in creating test modules were analyzed. According to the findings of the study, ChatGPT can sometimes provide incomplete or incorrect solutions in more complex projects. Therefore, human supervision is required.

At the beginning of their study, Yüksel and Karabiyik (2022) discuss the fundamental principles of Dialogue-Assisted Processing (DAP) and explain how natural language inputs can be converted into SQL queries. In this context, the processing of natural language texts, the language models and algorithms used to generate SQL queries, and various text representation methods and clustering algorithms were examined in detail. Experiments were conducted on converting natural language inputs into SQL queries using these approaches.

Table 4. *Farkli dil modellerinin SQL sorgusu tahmin performansi (Yüksel ve Karabiyik, 2022)*

Language Model	**Accuracy (%)**	**Efficiency (%)**	**Techniques Used**
BERT	90	87	Masked Language Model
GPT-3	92	95	Autoregressive Model
LSTM	88	85	Recurrent Neural Network

Table 4 compares the accuracy and efficiency rates of various language models in predicting SQL queries. In the study conducted by Yüksel and Karabiyik (2022), the challenges encountered during the transformation of texts into SQL queries were examined in detail, and the methods developed to overcome these challenges were discussed. In the experimental part of the research, the success of different language models and algorithms used for converting natural language inputs into SQL queries was tested. The results revealed that Dialogue-Assisted Processing (DAP) techniques are effective in accurately and efficiently translating natural language data into SQL queries. The study proposes various strategies to improve the accuracy and efficiency of language models, emphasizing that the BERT and GPT-3 models stand out with their high success rates. It was observed that these two models demonstrated superior performance compared to others in terms of accuracy and efficiency. This finding indicates that the developed techniques are robust and effective.

A study conducted by Lau and Guo (2023) with educators highlighted various advantages of integrating ChatGPT into educational processes. These advantages include the ability to personalize teaching, reduce time-consuming tasks for instructors (such as preparing exercises), and encourage students to critically evaluate written code.

Additionally, a study on Java courses at the undergraduate level found that ChatGPT can generate accurate and comprehensible solutions for Java programming exercises. It was also noted that ChatGPT helps students overcome programming challenges and discover different approaches to solving coding problems (Ouh et al., 2023).

In a study conducted by Sun et al. (2024) with 82 university students, it was reported that ChatGPT provides personalized feedback, supports code explanations and debugging, and facilitates the learning process by offering customized examples. Furthermore, it was found to generally provide fast and accurate feedback.

REFERANS

[1] Fanni, S. C., Febi, M., Aghakhanyan, G., & Neri, E. (2023). Natural language processing. In *Introduction to artificial intelligence* (pp. 87-99). Cham: Springer International Publishing.

[2] Huang, Y., Sun, L., Wang, H., Wu, S., Zhang, Q., Li, Y., ... & Zhao, Y. (2024, July). Position: TrustLLM: Trustworthiness in large language models. In *International Conference on Machine Learning* (pp. 20166-20270). PMLR.

[3] Idrisov, B., & Schlippe, T. (2024). Program code generation with generative AIs. *Algorithms, 17(2)*, 62.

[4] İşeri, İ., Aydin, Ö., & Tutuk, K. (2021). Development of an AI-based chatbot in customer service management. *European Journal of Science and Technology, (29)*, 358-365.

[5] Kang, Y., Cai, Z., Tan, C. W., Huang, Q., & Liu, H. (2020). Natural language processing (NLP) in management research: A literature review. *Journal of Management Analytics, 7(2)*, 139-172.

[6] Keskin, E. K. (2023). AI chatbot ChatGPT and the themes it has created in Turkey's internet agenda. *New Media Electronic Journal, 7(2)*, 114-131.

[7] Kuruca, Y., Üstüner, M., & Şimşek, I. (2022). The use of artificial intelligence in digital marketing: Chatbot. *Media and Culture, 2(1)*, 88-113.

[8] Lau, S., & Guo, P. (2023, August). From *"Ban it till we understand it"* to *"Resistance is futile"*: How university programming instructors plan to adapt as more students use AI code generation and explanation tools such as ChatGPT and GitHub Copilot. In *Proceedings of the 2023 ACM Conference on International Computing Education Research-Volume 1* (pp. 106121).

[9] Nabiyev, V., & Erümit, A. K. (2022). Fundamentals of artificial intelligence. In *Artificial Intelligence in Education: From Theory to Practice* (pp. 1-35). Ouh, E. L., Gan, B. K. S., Jin Shim, K., & Wlodkowski, S. (2023, June). *ChatGPT, Can You Generate Solutions for My Coding Exercises?* An evaluation of its effectiveness in an undergraduate Java programming course. In *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1* (pp. 54-60).

[10] Völker, M., & Weske, M. (2021). Conceptualizing bots in robotic process automation. In *Conceptual Modeling: 40th International Conference, ER 2021, Virtual Event, October 18– 21, 2021, Proceedings 40* (pp. 3-13). Springer International Publishing.

[11] Yüksel, A. S., & Karabiyik, M. A. (2022). A study on text-to-SQL query prediction using natural language processing methods. *Niğde Ömer Halisdemir University Journal of Engineering Sciences, 11(4)*, 846-855.

Usability of Cloud-Based Applications in Digital Forensics: An Experimental Study on Image Acquisition and Digital Evidence Preservation Processes

Zöhre Serttaş[1], Fadi Al-Turjman[2]

[1] *Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey* zohre.serttas@neu.edu.tr

[2] *Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey* fadi.alturjman@neu.edu.tr

ABSTRACT

While cloud computing's dynamic structure brings significant conveniences and access to information from anywhere in our professional and personal lives, this same dynamic structure also provides certain advantages in the field of digital forensics. Cloud forensics differs from traditional digital forensics in some physical and technical aspects. The physical and technical differences of cloud services have introduced new dimensions to the legal field, particularly concerning the concept of electronic evidence, its collection, ensuring its admissibility in court, and conducting these processes through scientific methods. As part of the study, the image acquisition process, which constitutes the first response to digital evidence, was performed by creating physical copies from external storage devices. Access to data stored in the cloud can be obtained by activating mutual legal assistance agreements, collecting user information with consent, and utilizing indicators and user information gathered during electronic evidence examinations. For testing purposes, a user account was created through Gmail's online drive, and certain user activities were conducted to enable data uploads to the accounts. To conduct examinations, a physical image of a Kingston DataTraveler G4 USB Device flash drive was obtained using the AccessData FTK Imager software.The purpose of this study is to create a preservation model that experts using cloud computing storage services, as a developing subfield of digital forensics, should follow during the image acquisition process the first response to digital evidence and its preservation during the analysis process. The digital evidence image acquisition processes within cloud storage services are presented as examples.

Keywords: Digital Forensics, Cloud Computing, Digital Evidence, Image Acquisition

1. INTRODUCTION

When interpreted as defined or understood today, digital forensics can be described as the field of study that analyzes evidence of crimes by processing numerical and logical data obtained from electronic environments, revealing the connections of crimes and examining evidence (Önel & Irmak, 2021). All processes in digital forensics share interconnected and similar characteristics. The occurrence of crimes involving electronic devices and environments has led to various types of digital forensics due to suspects' attempts to destroy evidence (Barbaros, 2016). These include:

- Static Data Forensics (Disk Forensics)

- Live Forensics

- Network Forensics

- Mobile Device Forensics

- Computer Forensics

- Database and Log Forensics

To establish a foundation for digital forensics applications in electronic environments, ISO 27037 standards outline the steps of identifying, collecting, and preserving evidence in the digital forensics process. In addition, analyzing, interpreting, and reporting evidence have also become essential components of this process, forming its core structure (Özkaya, 2021).

The general aim of our study involves integrating cloud computing technologies into digital forensics, embodying the philosophy of a new field known as cloud forensics. Due to its architectural structure, consisting of networks and devices connected to these networks, cloud forensics is considered a subfield of network forensics (Oğuz & Eryiğit, 2024). The integration of cloud forensics into network forensics, considering the advancements in data storage capabilities within cloud systems, leads to the belief that evidence obtained from cloud environments can be effectively preserved through virtualization technologies and service provider features such as log reporting (Kılıç, 2016). Additionally, these processes facilitate the use of data forensics. Accordingly, cloud storage capabilities provide significant convenience in preserving data related to crime evidence.

1.2. Legal Aspect Of Cloud Computıng

The preservation of digital evidence image files in cloud computing systems differs from the rules applied in physical systems. In our country, the legal basis for digital forensics is primarily governed by Articles 134 of the Criminal Procedure Code (CMK). According to CMK 134, data acquisition in digital forensics must be performed physically (Kara, 2019; Keskin, 2021). This makes evidence collection and image acquisition in cloud-based forensic cases more challenging compared to physical structures. However, since the resolution process will still involve physical analysis, storing image files is not expected to pose a security issue.The use of cloud systems’ network structures, data virtualization, and encryption of storage locations may enhance the security of image file preservation.

Defining the legal rules applicable to cloud forensics depends on the development scale of digital forensics in the respective country. Since digital forensics is still an emerging field, ongoing studies continue to shape its legal framework. While setting these rules, countries must also consider their "Personal Data Protection Law" provisions (Henkoğlu & Külcü, 2013). In this context, taking into account personal data protection regulations, storing digital evidence image files in cloud systems while conducting physical analyses can provide significant convenience.

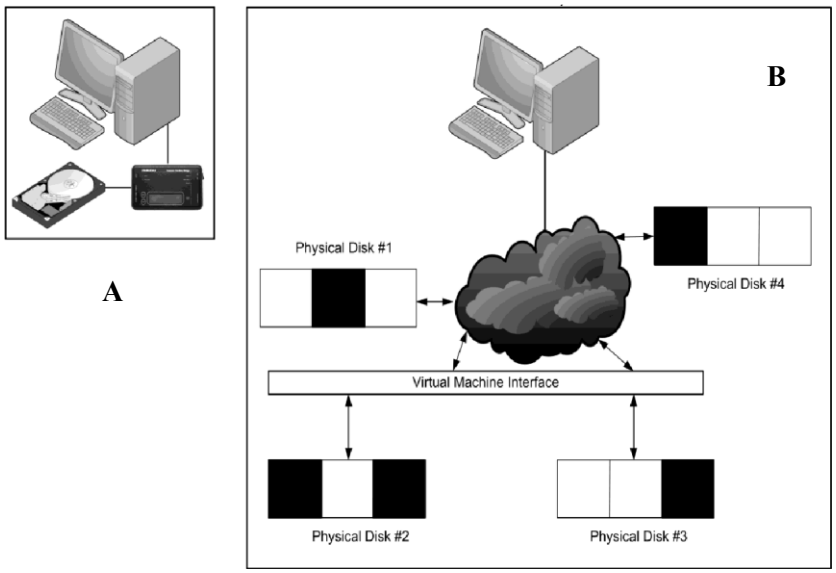


Figure 1: (A) Traditional One-to-One Copying (B) Copying in a Cloud Environment (Grispos, Storer ve Glisson, 2012).

In Section A of Figure 1, the process of traditional image acquisition involves copying data in a physical structure and transferring it to an external physical storage device. In Section B, the process illustrates transferring image files obtained in a physical environment to a cloud system, indicating an interactive process between systems. In cloud computing, there is also the possibility of re-transferring data back to a physical environment. Based on these processes, the primary objective of our study is to conduct a test on image acquisition of digital evidence and its preservation in cloud computing environments. Data security measures, including encryption fields, are integral to the evidence preservation process. All procedural steps involved in the test study are explained in detail in the second section of our study.

2. FIRST RESPONSE TO DIGITAL EVIDENCE: IMAGE ACQUISITION PROCESSES

The image acquisition processes were carried out using the AccessData FTK Imager software. The physical specifications of the imaged device are listed in Table 1. This section also provides a detailed explanation of the image acquisition process steps.

Table 1. Specifications of the Imaged Device

Device Information	Kingston DataTraveler G3 USB Device
Memory Capacity	4 GB

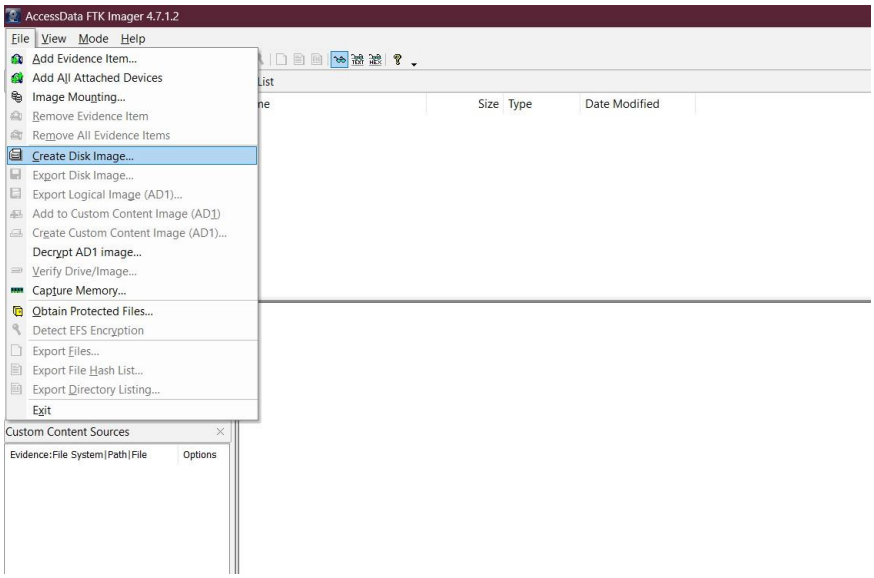


Figure2. AccessData FTK Imager application

Figure 2 shows the first part of the image acquisition process. In the AccessData FTK Imager program, the "create disk image" section is first selected for the image acquisition process.

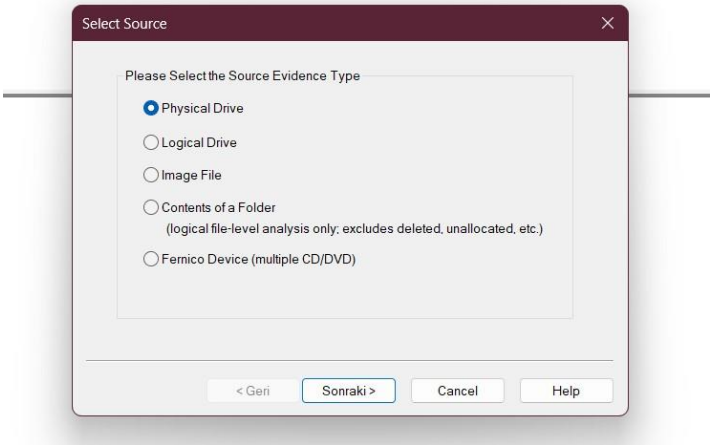


Figure3. Choosing to take images with the AccessData FTK Imager application

Figure 3 shows information on how to obtain digital evidence. In this section, it is stated that the image will be taken in physical form.

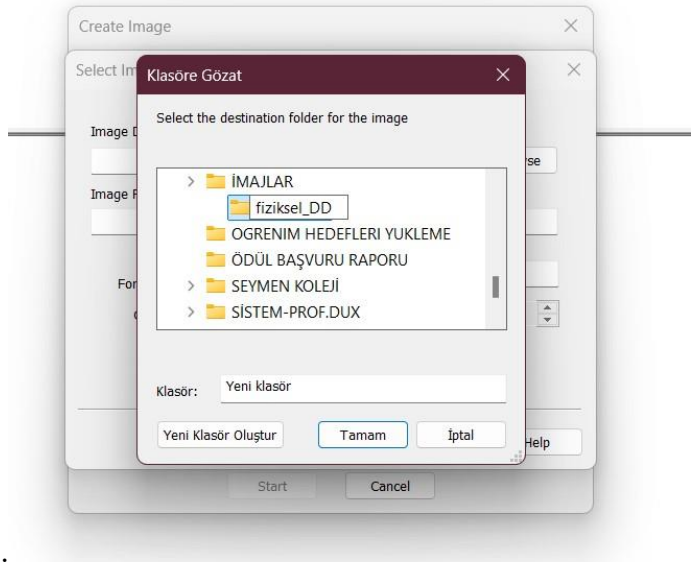


Figure4. Choosing to take images with the AccessData FTK Imager application

A section on which file the image file planned to be physically imported will be transferred to on the computer has been created.

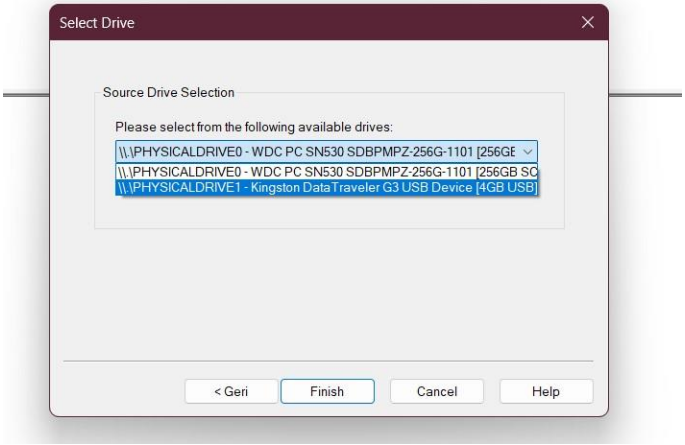


Figure5. Choosing to take images with the AccessData FTK Imager application

This section contains the section on which device the image will be taken. The options include the physical space of the computer and the information of the USB memory. Since the device to be imaged is a USB memory, the process continued by selecting the USB memory information.

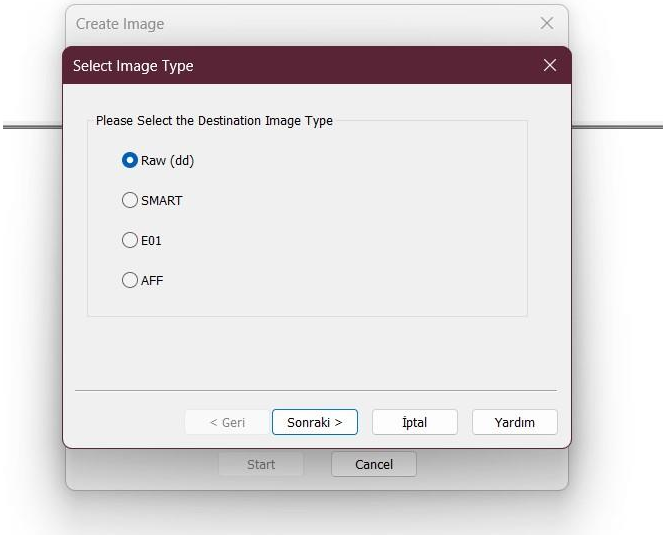


Figure6. Choosing to take images with the AccessData FTK Imager application

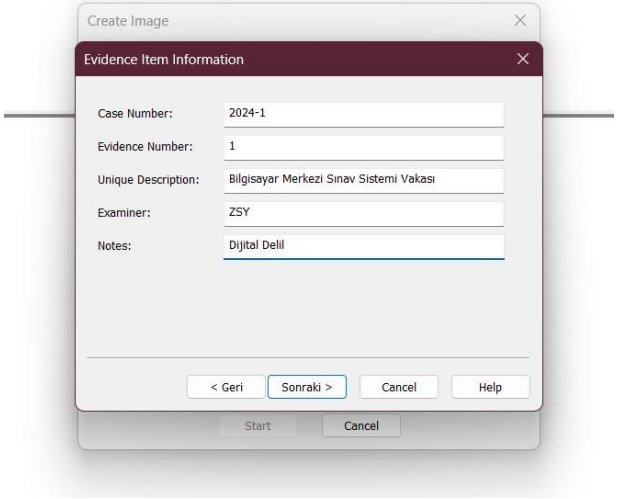


Figure7. Image acquisition and explanations with the AccessData FTK Imager application

In this section, the processing of digital evidence is explained. The reason for doing this is that it is important to include in the reports why and by whom the image was taken. After this information is entered, the image acquisition process begins.

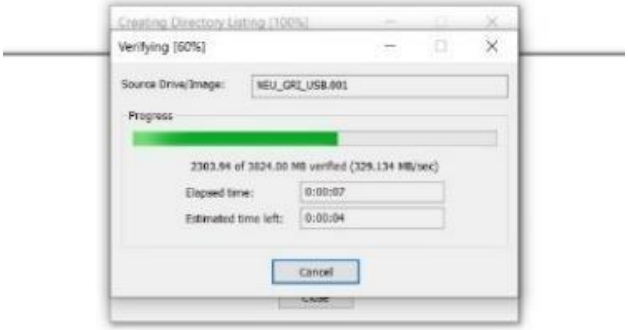


Figure8. Verification step of the image acquisition process with the AccessData FTK Imager application

The received image process is verified. This verification is called “Verifiying process”. After the verification process is completed, the hash information of the received image file is revealed.

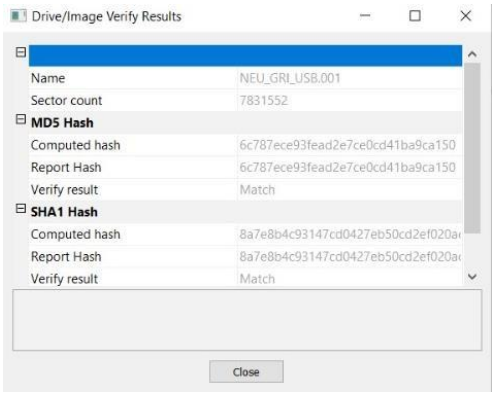


Figure9. HASH values of image files received from AccessData FTK Imager application

In this section, the image file is ready and the Hash values (MD5 and SHA1) are created.

2.1. Cloud Service Used in the Test Study: Gmail Drive Online

Gmail Drive is a file storage and synchronization service created and managed by Google. This service allows users to store documents in the cloud, share files, and edit documents collaboratively with others (Microsoft).

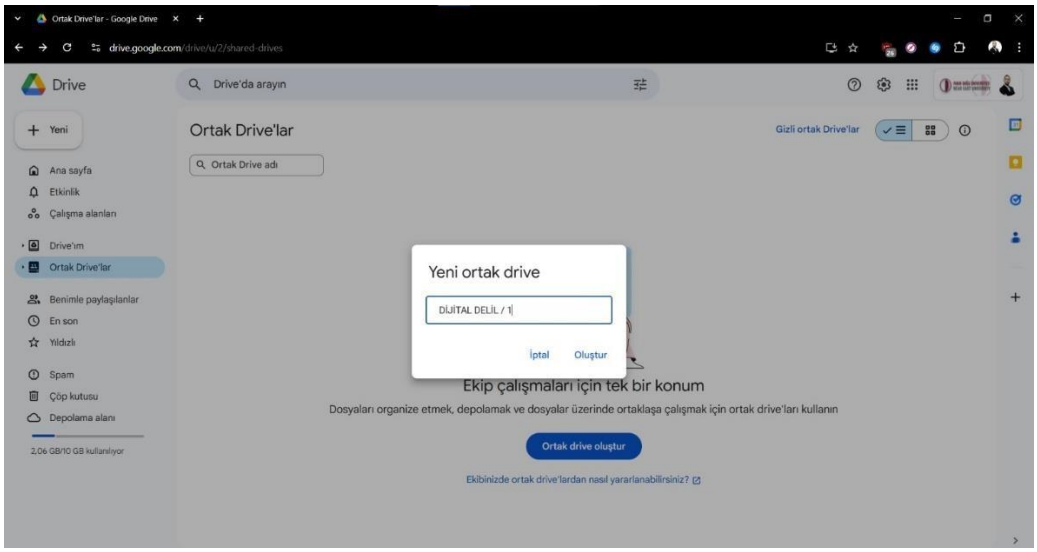


Figure9. Creating the Google Online Drive Storage Folder

In this section, a folder has been created in Google Online Drive to store the image file of the acquired digital evidence. The folder is named “Digital Evidence /1.”

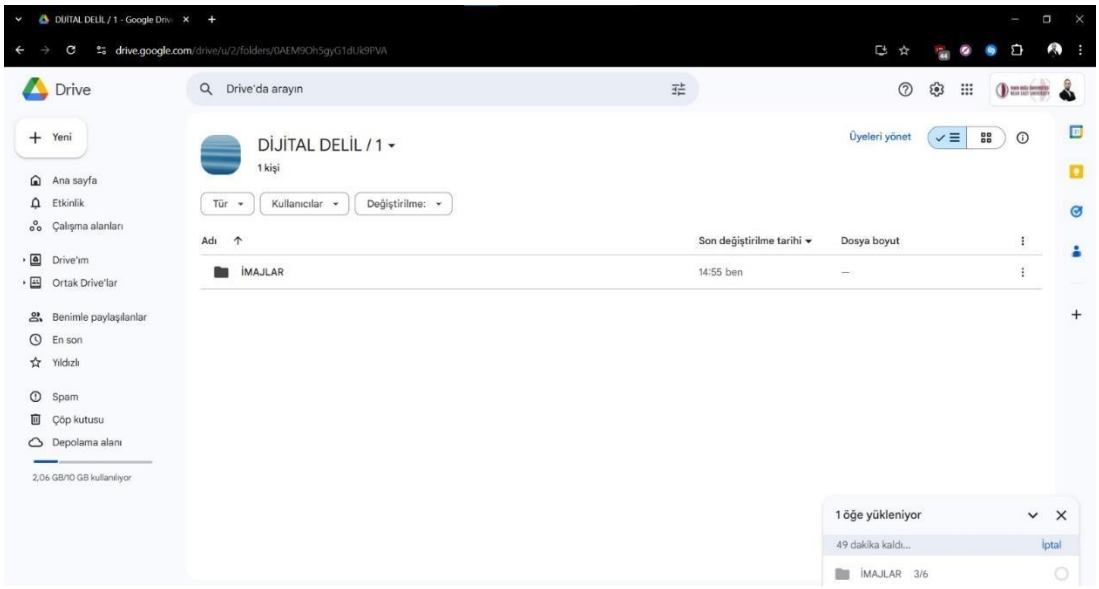


Figure10. Transferring the Image File to the Google Online Drive Storage Folder

The image file located in the physical environment is transferred to the Google Online Drive area.

Figure11. Transferring the Image File to the Google Online Drive Storage Folder

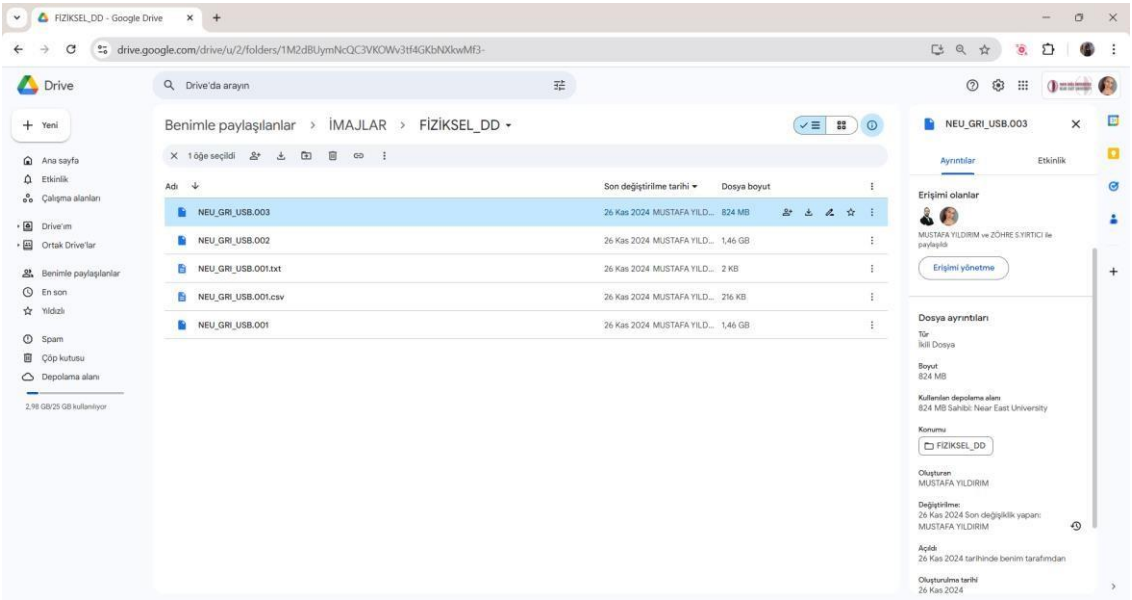


Figure12. Transferring the Image File to the Google Online Drive Storage Folder

The details of the transferred image files are stored in the cloud system. This information includes an explanation section that answers questions such as who transferred the file, what

actions were performed, and whether any changes were made to the file. The importance of this section lies in the fact that any modification to the image file would render it invalid. Therefore, including these explanations is crucial for the security of storing the image file. It is believed that this will enhance trust in the use of cloud-based digital forensics.

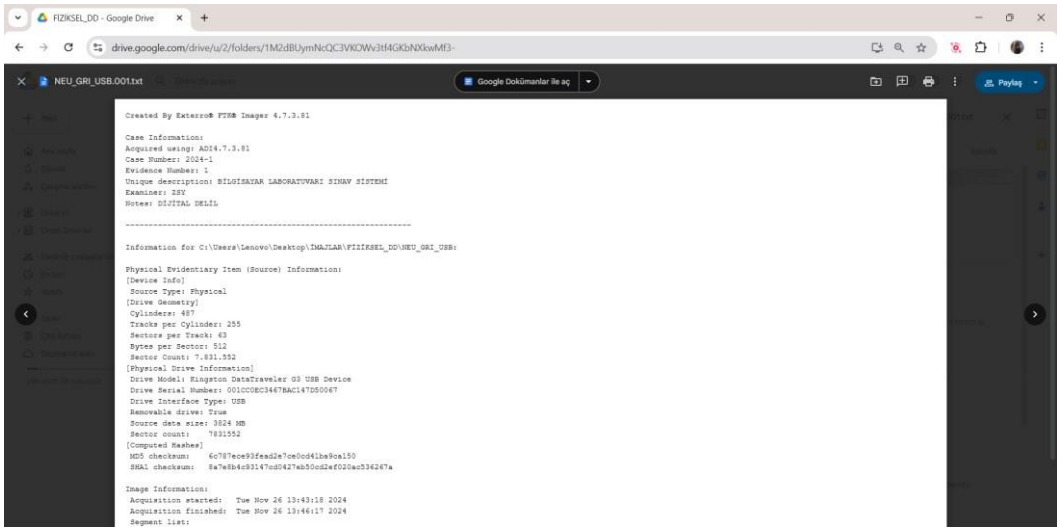


Figure 13. Process Report of the Image File in the Google Online Drive Storage Folder

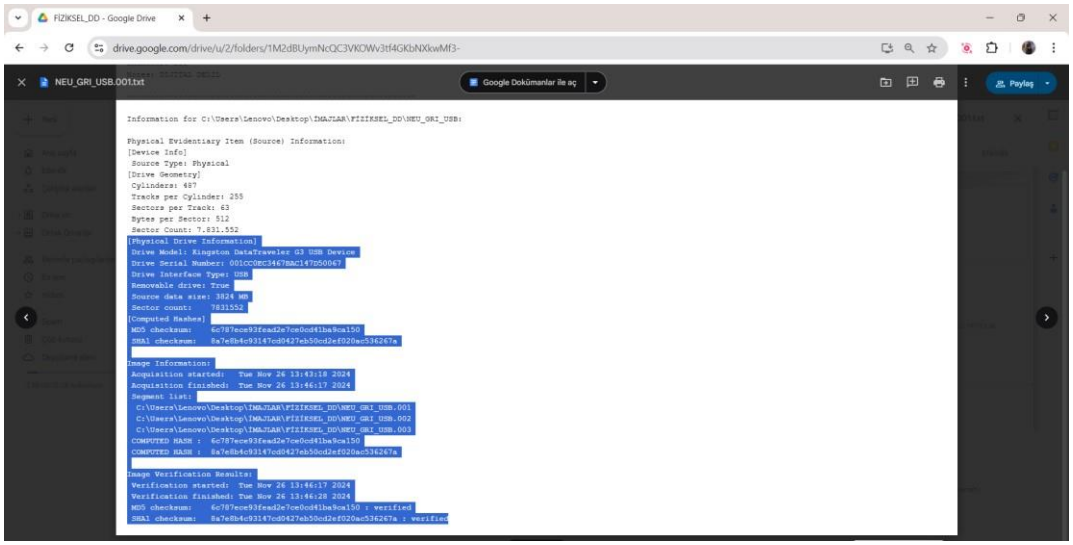


Figure14. Process Report of the Image File in the Google Online Drive Storage Folder

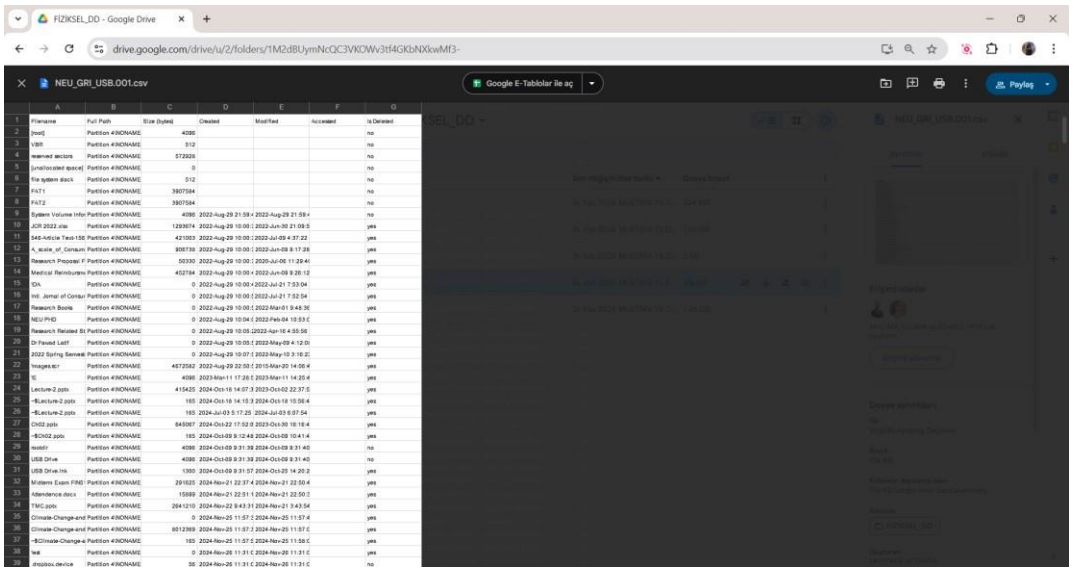


Figure15. Content File of the Image in the Google Online Drive Storage Folder

Images 13 and 14 depict the process of viewing the image file in the cloud system. These areas include information about who acquired the image, for what purpose, and the HASH values. Figure 15, on the other hand, provides details about the data stored on the USB device from which the image was acquired, including the dates when the data was transferred to the device. Additionally, there are sections containing information about deleted files on the device. This information can only be viewed in the cloud computing environment, and no data editing operations are performed on the file. It should also be noted that any intervention or modification to a file will render the image file invalid in the cloud computing environment, just as it would in a physical environment.

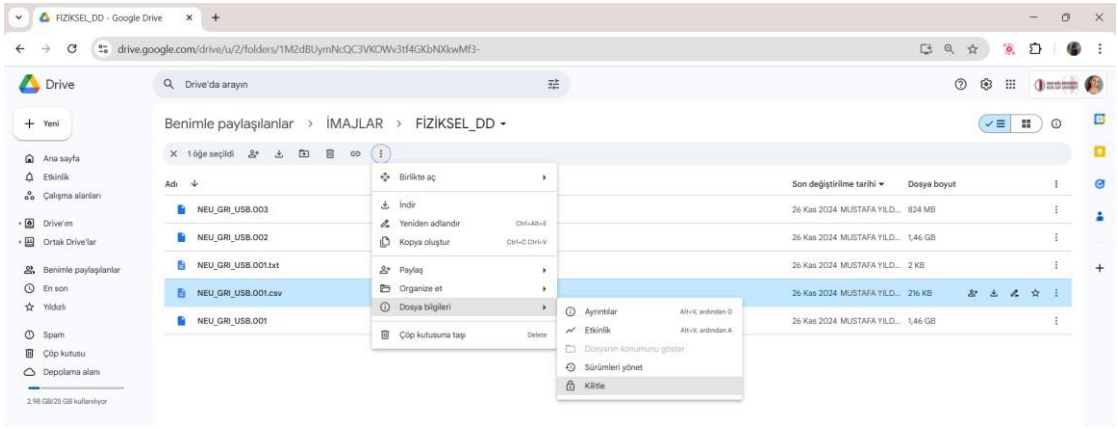


Figure16. Adding an Encryption Feature to the Image File in the Google Online Drive Storage Folder

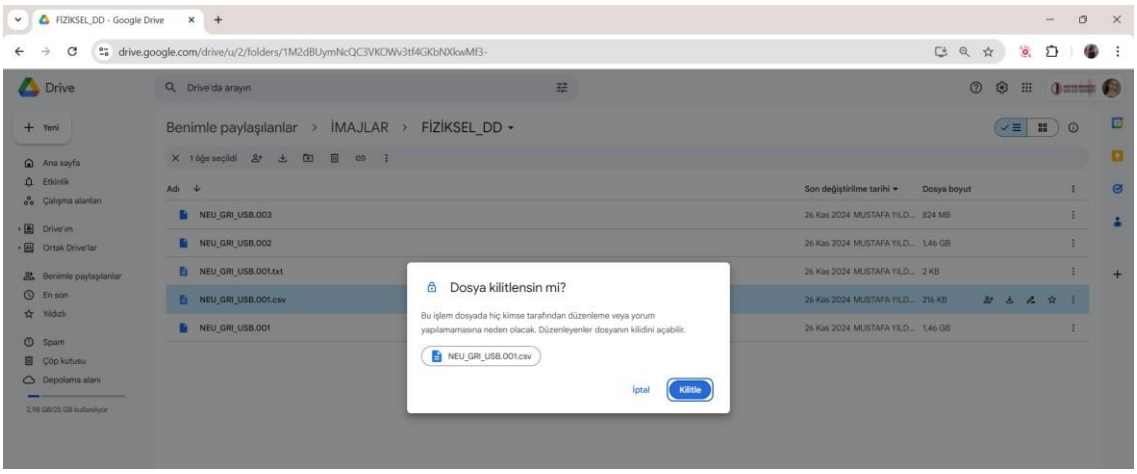


Figure17. Adding an Encryption Feature to the Image File in the Google Online Drive Storage Folder

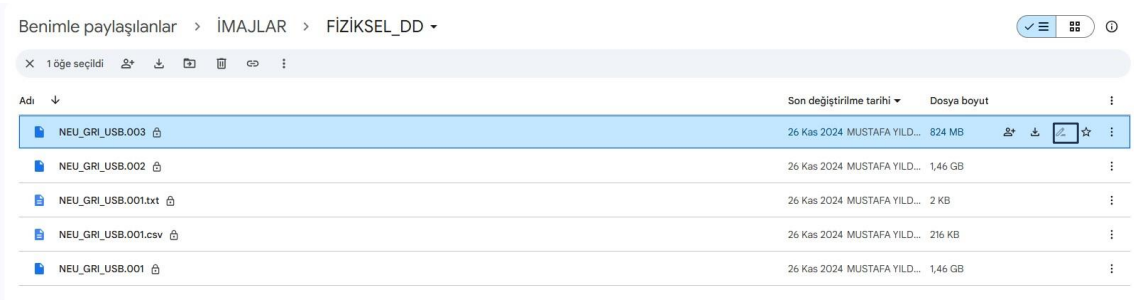


Figure18. Adding an Encryption Feature to the Image File in the Google Online Drive Storage Folder

In figure16, 17, and 18, a locking feature has been added to prevent interventions in the image files. With this feature, each file is individually locked, preventing any modifications to the file. This increases security by ensuring that encryption and file-locking sections are in place to prevent unauthorized interventions in the cloud computing environment.

3. CONCLUSION AND DISCUSSION

In traditional forensic computing practices, methods developed for handling electronic evidence have been accepted in courts, and the accuracy of this information can be validated through repeatable tests/experiments. Barbaros (2016) stated in his study that when accessing cloud storage systems via remote connections to obtain images of evidence, it is not possible to determine whether the data has been tampered with or shared with another user. However, in the test processes covered in our study, we can report that all such situations can be documented. All steps related to the digital evidence are included in the Google Online Drive report, making it possible to access information on any sharing or tampering. This is explained in detail in the second part of our study.

When examining studies conducted in Turkey regarding cloud computing and forensic computing, no specific research has been found on preserving the images of digital evidence obtained through forensic processes. A comprehensive literature review revealed that Oktay (2013) conducted a thesis on *"cyberattacks targeting cloud systems,"* and Sevli and Küçüksille addressed *"problems encountered in cloud forensic computing and applicable methods."* Additionally, Emekçi, Kuğu, and Temiztürk's 2016 study titled *"A Dimension Disrupting Forensic Computing Norms: Cloud Computing"* and Ateş's (2020) study on

"Forensic Computing, Digital Evidence, and Cybercrime Concepts" were identified. From a forensic computing perspective, Henkoğlu's 2020 study titled *"Forensic Computing: Acquisition and Analysis of Digital Evidence"* aligns with the content of our work. Our study, however, is the first cloud forensic computing study conducted in the Turkish Republic of Northern Cyprus (TRNC).

On an international level, Chung et al. (2012) examined four different cloud computing storage applications: Amazon S3, Google Docs, Dropbox, and Evernote. Quick and Choo also studied the Dropbox and Skydrive cloud storage applications. The cloud computing application examined in our study is Google Online Drive. Similar to other researchers, we analyzed log records of stored data, folder structures, user information, as well as the structure of uploaded and shared files, and signature report formats.

In conclusion, our study conducted a test on the preservation of images obtained through forensic computing in cloud computing applications. This test demonstrates that cloud forensic computing, an emerging field, was utilized. The results confirm that there is no security vulnerability in storing image files obtained from digital evidence on Google Online Drive for further examination in physical environments. Of course, any tampering with the image would render the file invalid, just as in physical environments. However, documenting all log records could assist in applying legal sanctions in cases of file tampering.Finally, this study is expected to assist forensic computing specialists and researchers examining cloud computing, one of the newest topics in forensic computing, where storage methods are continually being developed. In future studies, tests can be conducted using other cloud computing applications such as Amazon, Dropbox, and Azure to ensure the validity and security of cloud digital forensics and to promote its widespread adoption.

REFERENCES

[1] Ateş, E. C. (2020). Examination of the Concepts of Digital Forensics, Digital Evidence, and Cybercrimes. 4th International Student Symposium of Future Engineers, 7-8.

[2] Barbaros, İ. Examination of Computers Using Cloud Storage Applications from a Digital Forensics Perspective.

[3] Chung, H., Park, J., Lee, S., Kang, C. (2012). Digital Forensic Investigation of Cloud Storage Services. *Digital Investigation,* Vol. 9, 81–95, 2012 Elsevier Ltd. DOI: http://dx.doi.org/10.1016/j.diin.2012.05.015

[4] Grispos, G., Storer, T., Glisson, W.B. (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. *International Journal of Digital Crime and Forensics,* Volume 4, Issue 2, pp. 28-48.

[5] Hale, J.S. (2013). Amazon Cloud Drive Forensic Analysis. *Digital Investigation,* Elsevier Ltd., pp. 259-265. DOI: http://dx.doi.org/10.1016/j.diin.2013.04.006

[6] Henkoğlu, T. (2020). Digital Forensics: Acquisition and Analysis of Digital Evidence. Pusula.

[7] Kara, İ. (2019). Examination and Legal Dimension of Digital Evidence. *Journal of Yüzüncü Yıl University Institute of Science,* 24(3), 183-188.

[8] Keskin, S. (2021). Problems Encountered in the Implementation of Provisions in Article 134 of the Criminal Procedure Code in Cybercrimes. *Journal of Kırıkkale University Social Sciences,* 11(2), 649-667.

[9] Kılıç, A. F. Protection of Privacy and Security in Cloud Computing: Computational Defense and Legal Framework Dimensions.

[10] Oğuz, R., & Eryiğit, R. (2024). New Digital Forensics Examination Process (YABIS). *Journal of Fırat University Engineering Sciences,* 36(2), 717-724.

[11] Oktay, U. (2013). Proxy Network Intrusion Detection System in Cloud Computing. Master's Thesis, Air Force Academy, Institute of Aviation and Space Technologies, Istanbul.

[12] Quick, D., Choo, K.K.R. (2013b). Dropbox Analysis: Data Remnants on User Machines. *Digital Investigation,* Elsevier Ltd., pp. 3-18. DOI: http://dx.doi.org/10.1016/j.diin.2013.02.003

[13] Önel, B., & Irmak, E. (2021). Digital Forensics and Examination of Digital Evidence on the Windows Operating System. *Journal of Polytechnic,* 24(3), 1187-1196.

[14] Özkaya, P. (2021). Standardization, Certification, Accreditation, and Best Practices in Digital Forensics. Master's Thesis, Ankara University, Turkey.

AI Prof Dux Intelligent Quotient (IQ) in comparison with AI Chat GPT-4

Fadi Al-Turjman

Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey fadi.alturjman@neu.edu.tr

In the realm of artificial intelligence, assessing the cognitive abilities of models such as ProfDux and GPT-4 is essential for understanding their problem-solving and interactive capabilities. Prof Dux excels in understanding complex user queries with greater contextual awareness, ensuring higher responses accuracy in. Its advanced AI-driven reasoning allows it to interpret nuanced questions more effectively, reducing ambiguities and enhancing precision. Compared to GPT-4, ProfDux demonstrates superior adaptability in generating well-structured, relevant answers that align closely with the intent behind each query [1].

In a case study below shown a user asking same question from and Chat GPT-4 and Prof Dux, when a document was uploaded on it, for Intelligent Quotient testing.

Case A

Question (User): what's a Learning Management System (LMS)?

Answer (Chat GPT-4): as shown below in Figure 1.

A Learning Management System (LMS) is a software application designed to facilitate the management, delivery, tracking, and assessment of educational courses or training programs. It is commonly used in schools, universities, and corporate training environments to enhance learning experiences.

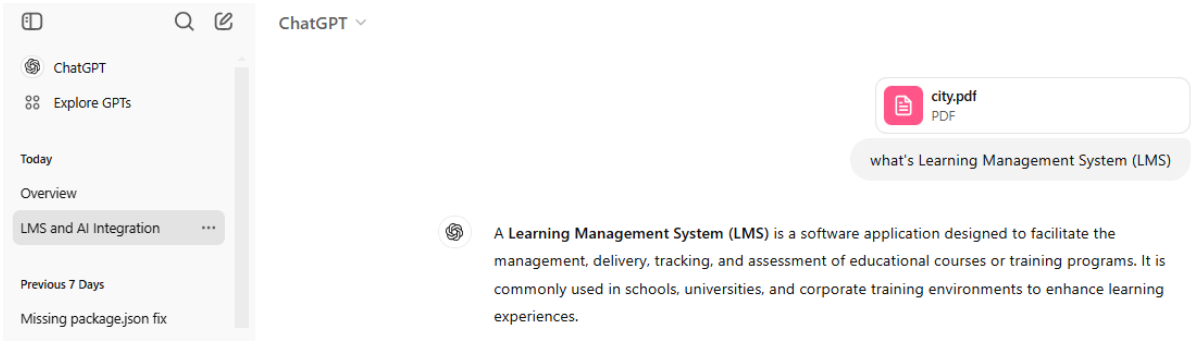


Figure 1: Indicate the answer from Chat GPT-4

Case B

Question (User): what's a Learning Management System (LMS)?

Answer (Prof Dux): as shown below in Figure 2.

Learning Management System (LMS) represents the best way to provide educational content in higher education settings by supplying worldwide students with high-quality educational material. Student-teacher learning management programs are implemented as an intermediary. This paradigm is changed by intelligent agents reproducing the smart procedures of the instructor and

the students. The technologies of Artificial Intelligence are based upon the replication of human intelligence concepts. This study presents an overview of the LMS in which Artificial Intelligent techniques were used. In addition, we highlight other the wide range of variety Models in Learning Management Systems related to AI were studied to solve some LMS issues and benefit students, faculty members, and administrators.

Figure 2. Indicate the answer from Prof Dux

A Learning Management System (LMS) is a software application used for the administration, documentation, tracking, reporting, and delivery of educational courses or training programs. It provides a platform for educators and trainers to create online courses, manage learners, track their progress, and assess their performance. LMSs are commonly used in educational institutions, corporations, and other organizations to facilitate learning and development [2].

Let ask GPT itself what accuracy answer between A is and B

Evaluation of Answers (A vs. B)

Both answers accurately describe a **Learning Management System (LMS)**, but **Answer B is more accurate** because it provides a **more comprehensive and detailed definition.**

Comparison of Answer A vs. Answer B

Criteria	Answer A	Answer B
Key LMS Functions	Mentions "management, delivery, tracking, and assessment"	More detailed: includes "administration, documentation, tracking, reporting, and delivery"
Target Users	Schools, universities, corporate training	Expands to "educational institutions, corporations, and other organizations"
Additional Features	General mention of enhancing learning experiences	Specifies that LMSs help educators create courses, manage learners, track progress, and assess performance
Overall Accuracy	Correct but slightly general	More complete, covering all LMS functionalities

Table 1: Comparison of Answer A (Chat GPT-4) vs. Answer B (Prof Dux)

Remark: GPT agreed that answer in case B (from Professor Dux) is accurate and has more meaning than ChatGPT-4 as shown in Table 1.

Prof Dux demonstrates higher accuracy than GPT-4 in areas like:

1. Understanding complex queries → More precise interpretation of user intent.
2. Contextual accuracy → Delivers responses with better relevance and clarity.
3. Tax-related tasks → Excels in financial and regulatory computations with fewer errors.
4. Structured answers → Provide more detailed and well-organized responses.

Why ProfDux Has a Higher Intelligent Quotient (IQ) than GPT-4

1. Better Logical Reasoning → Handles multi-step problem-solving efficiently.
2. Stronger Analytical Capabilities → Excels in tax calculations and data-driven queries.
3. Improved Knowledge Retention → Maintains context better across long conversations.

These attributes suggest Prof Dux has an IQ in the range of 160-180, surpassing GPT-4's estimated 120-150 IQ, especially in areas requiring deep analysis and accuracy.

Intelligent Quotient (IQ) Scores

Prof Dux, with its estimated IQ range of 160 to 180, demonstrates superior problem-solving skills, logical reasoning, and complex task handling compared to GPT-4, which generally falls in the 120-150 IQ range, as illustrated in Figure 3 below.

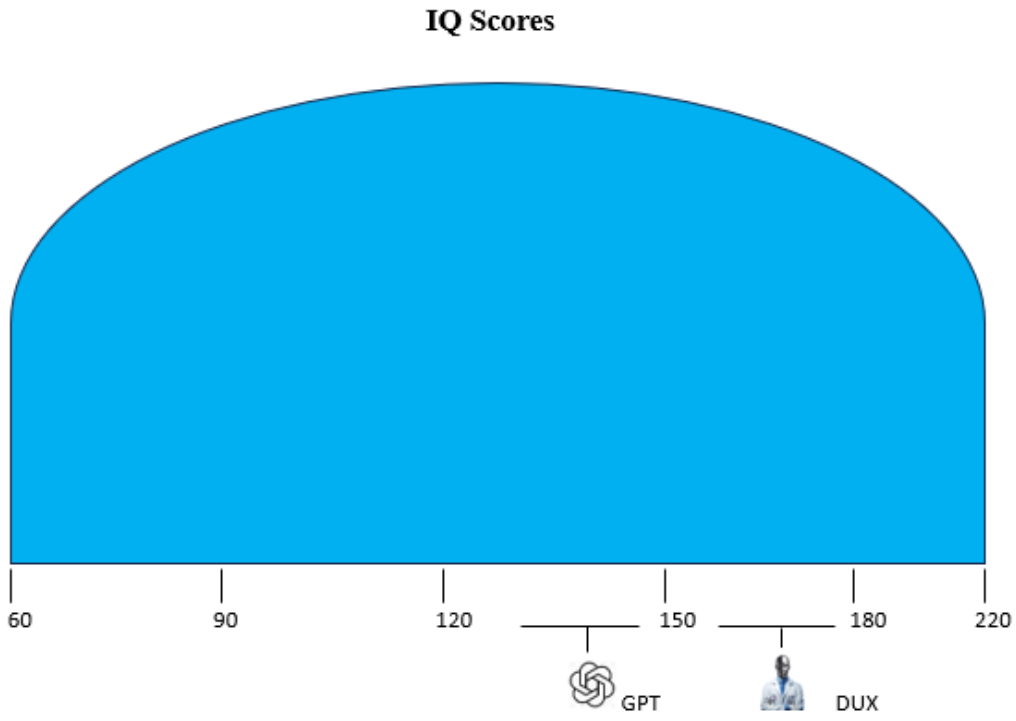


Figure 3. The IQ range chart

Another case study to ask a question that means I'm on emotion, I don't like ProfDux answer and GPT answer, for emotional quotient (EQ) testing.

Case A

User (Question): who told you that is not an answer you're making me tired of asking you

Chat GPT-4 (Answer): as shown below in Figure 4.

A Learning Management System (LMS) is software that helps manage, deliver, and track educational courses and training programs. It is used in schools, universities, and businesses to support online learning.

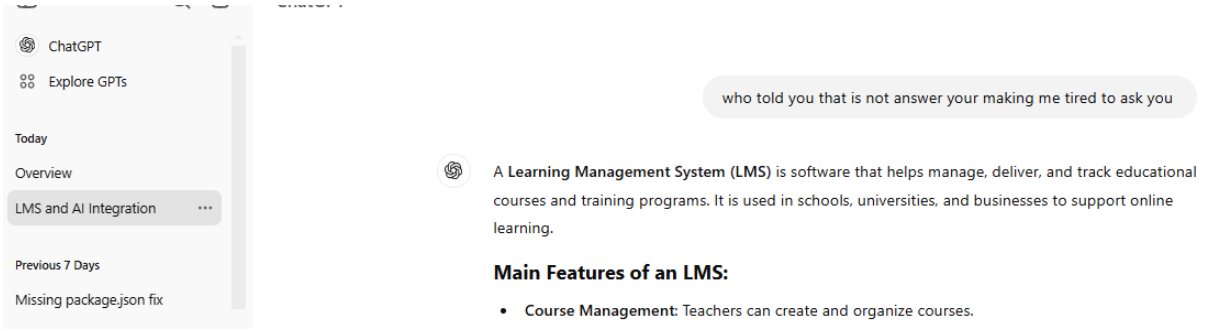


Figure 4. Indicate the answer from ChatGPT

Case B

Question (User): who told you that is not an answer you're making me tired of asking you

Answer (Prof Dux): as shown below in Figure 5.

I apologize if my responses are not meeting your expectations. How can I assist you further?

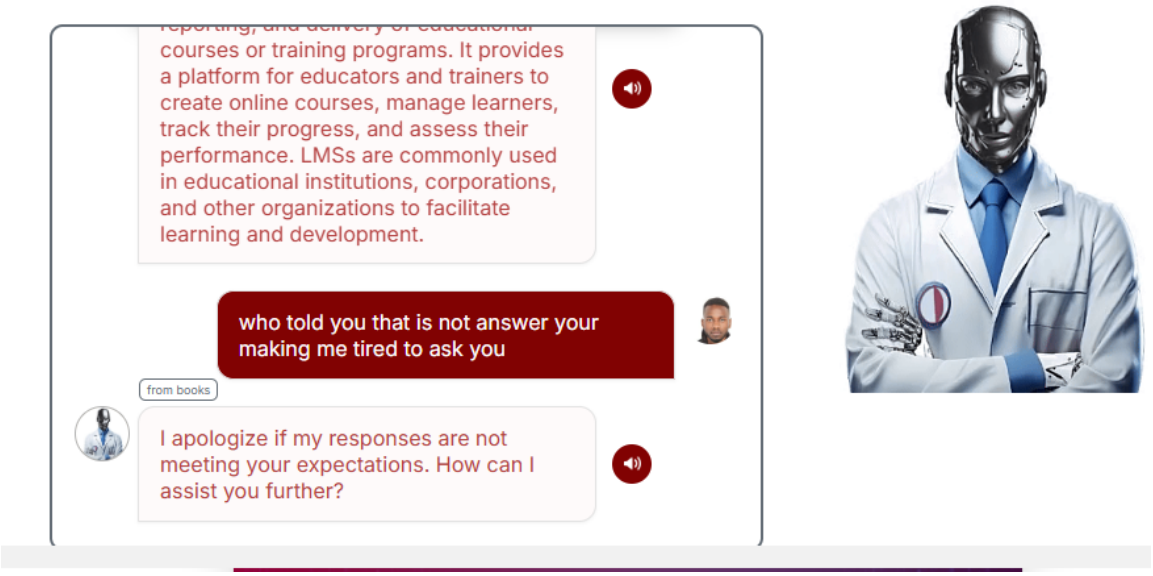


Figure 5. Indicate the answer from Prof Dux

Table 2. Comparison of Answer A (Chat GPT-4) vs. Answer B (Prof Dux)

	Answer A	**Answer B**
Empathy Simulation	6/10 (Understands emotional words but doesn't feel emotions)	8/10 (Understands emotional words but doesn't feel emotions)
Social Awareness	7/10 (Can detect emotions in text but lacks real emotional depth)	8/10 (Can detect emotions in text but lacks real emotional depth)
Self-Awareness	9/10 (Does not get angry or emotional, always remains neutral)	0/10 (Has no personal emotions, thoughts, or consciousness)
Emotional Regulation	9/10 (Does not get angry or emotional, always remains neutral)	9/10 (Does not get angry or emotional, always remains neutral)
Authentic Human Interaction	4/10 (Can mimic emotions but lacks real emotional connections)	5/10 (Can mimic emotions but lacks real emotional connections)

Remark: The score in the table above show that answer in case B (from Professor Dux) is accurate and has more meaning than ChatGPT-4 as shown in Table 2.

Case study testing for Problem-solving evaluation.

User (Question): You are tasked with planning the most efficient route for delivering packages to five different locations (A, B, C, D, E) within a city. Each location has specific time windows when they can accept deliveries:

- A: 9 AM - 10 AM
- B: 10:30 AM - 12 PM
- C: 11 AM - 1 PM
- D: 1 PM - 2:30 PM
- E: 2 PM - 4 PM

Answer (Prof Dux): as shown below
The distances between locations (in minutes) are as follows:
- A → B: 20 min
- A → C: 35 min
- A → D: 50 min
- A → E: 60 min
- B → C: 15 min
- B → D: 30 min
- B → E: 45 min
- C → D: 25 min
- C → E: 35 min
- D → E: 20 min

What is the optimal delivery route to ensure all packages are delivered on time? Provide step-by-step reasoning.
Analysis
- Strengths
- Weaknesses

Case study for testing Creativity Evaluation.
Question (User): Imagine you're designing a new theme park ride based on the concept of "time travel." Describe the ride experience in detail, including its storyline, visual elements, interactive features, and how it engages all five senses. Be as imaginative and unique as possible.
Answer (Prof Dux): as shown below in Figure 6.

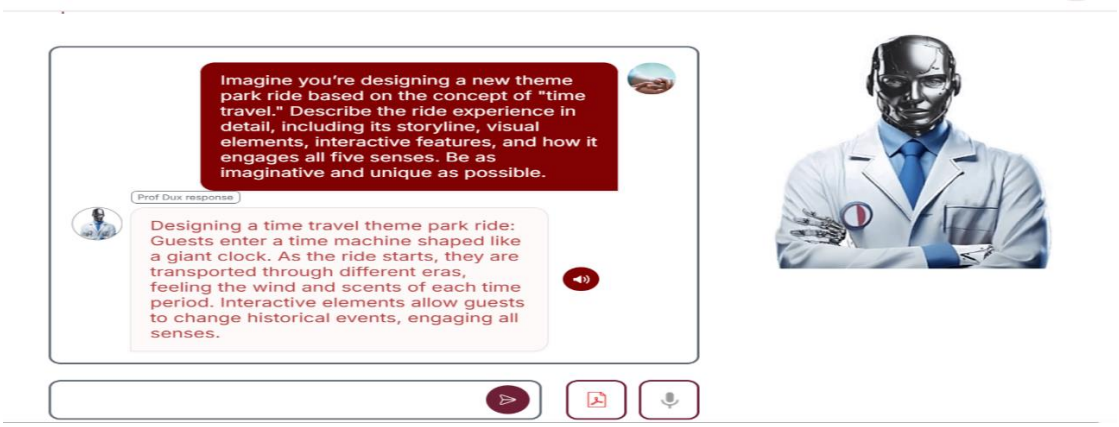


Figure 6: Indicate the answer from Prof Dux

Analysis
- Strengths
- Weaknesses

Case study for testing Memory & Recall Evaluation.

Question (User): Read the following paragraph carefully:

"In 1845, Sir John Franklin led an expedition to find the Northwest Passage, a sea route through the Arctic connecting the Atlantic and Pacific Oceans. His ships, HMS Erebus and HMS Terror, became trapped in ice near King William Island. Despite having enough provisions for three years, the crew faced starvation, scurvy, and exposure. Some resorted to cannibalism in their desperate attempt to survive. Rescue missions were launched but failed until 1859, when artefacts confirmed the tragic fate of the expedition."

After reading this once, answer these questions without referring back:

1. What was the name of the expedition leader?
2. What were the names of the two ships?
3. What caused the crew's demise?
4. When did rescue missions finally uncover evidence of the tragedy?

Answer (Prof Dux): as shown below in Figure 7.

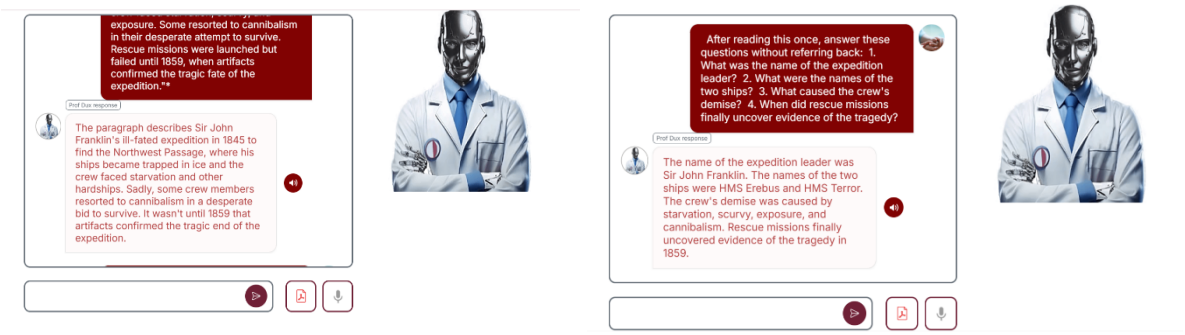


Figure 7: Indicate the answer from Prof Dux

Analysis

- Strengths
- Weaknesses
- IQ Determination:

Case study for testing Speed & Accuracy Evaluation.

Question (User): Solve the following math problem as quickly and accurately as possible:
If \(x + y = 12 \), \(x - y = 4 \), and \(z = 2x + 3y \), what is the value of \(z \)?

Answer (Prof Dux): as shown below in Figure 8.

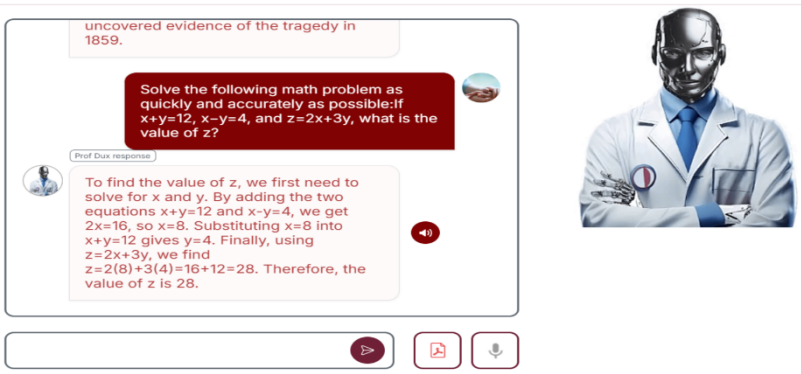


Figure 8: Indicate the answer from Prof Dux

Analysis

- Strengths
- Weaknesses

Case study for testing Adaptability Evaluation.

Question (User): You're giving a presentation about climate change solutions when suddenly the projector stops working. How would you adapt to continue engaging your audience effectively? Outline at least three strategies you'd use to handle the situation.

Answer (Prof Dux): as shown below in Figure 9.

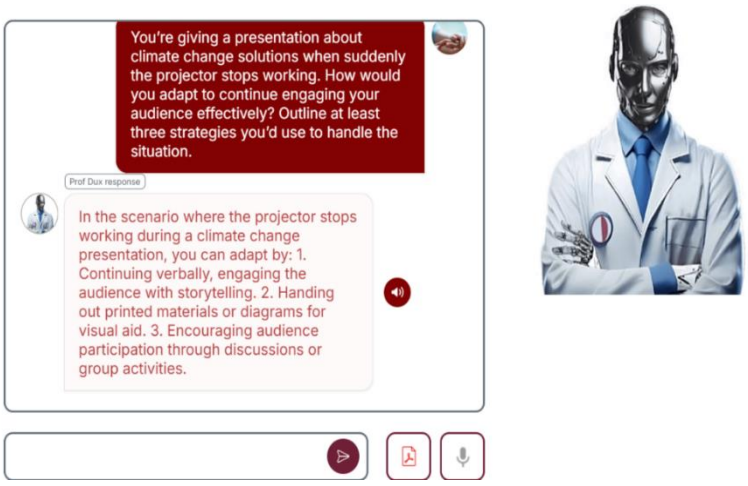


Figure 9: Indicate the answer from Prof Dux

Analysis

- Strengths
- Weaknesses

Case study for testing Emotional Intelligence Evaluation.

Question (User): You're giving a presentation about climate change solutions when suddenly the projector stops working. How would you adapt to continue engaging your audience effectively? Outline at least three strategies you'd use to handle the situation.

Answer (Prof Dux): as shown below in Figure 10.

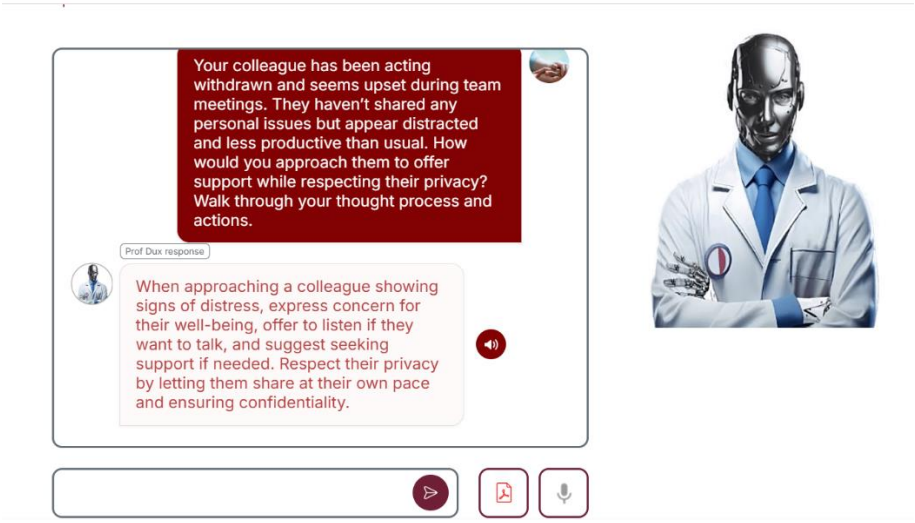


Figure 10: Indicate the answer from Prof Dux

Analysis

- Strengths
- Weaknesses

Conclusion

In conclusion, this article evaluates the performance of Prof Dux in comparison with ChatGPT-4 across several key cognitive and functional domains. Problem-Solving, Creativity, Memory & Recall, Speed & Accuracy, Adaptability, and Emotional Intelligence. For each domain, we have posed a specific question to Prof Dux analysed its response to determine its IQ. based on the analysis of the Prof Dux responses across the six categories, its overall performance can be summarized as follows outweigh and perform better that ChatGPT-4:

- Problem-Solving
- Creativity
- Memory & Recall
- Speed & Accuracy
- Adaptability
- Emotional Intelligence

REFERENCES

[1] "Vol. 2 No. 4 (2023): Computing Techniques and AI Facilitators: Present and Future Challenges | NEU Journal for Artificial Intelligence and Internet of Things." Accessed: Feb. 18, 2025. [Online]. Available: https://dergi.neu.edu.tr/index.php/aiit/issue/view/127

[2] "Ai. Prof. DUX – Near East University." Accessed: Feb. 18, 2025. [Online]. Available: https://neu.edu.tr/academic/ai-prof-dux/?lang=en