DAYANANDA SAGAR UNIVERSITY

KUDLU GATE, BANGALORE – 560068

Bachelor of Technology

in

CSE (AI&ML)

Introduction to Network & Cyber Security

Mini Project

"TEXT TO EMOJI ENCRYPTION AND DECRYPTION"

BY

ENG20AM0016 Bharath K
ENG20AM0022 Chandan Neralgi
ENG21AM0057 Kiran Immadi
ENG21AM0058 Dhanush.kolisetty

Under the supervision of

Prof. Pavithra Anjanappa
Associate Professor, Dept of CSE (AI & ML)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,

SCHOOL OF ENGINEERING DAYANANDA SAGAR UNIVERSITY,

(2023-2024)

DAYANANDA SAGAR UNIVERSITY

School of Engineering

Department of Computer Science& Engineering

Kudlu Gate, Bangalore –560068

Karnataka, India

CERTIFICATE

This is to certify that the INCS MINI PROJECT titled **"TEXT TO EMOJI ENCRYPTION AND DECRYPTION"** is carried out by Bharat K. **(ENG21AM0016),** Chandan Neralgi **(ENG21AM0022),** Kiran Immadi **(ENG21AMM0057),** Dhanush.kolisetty **(ENG21AM0058),** Bonafede students of Bachelor of Technology in CSE AIML at the School of Engineering, Dayananda Sagar University, Bangalore in partial fulfilment for the award of degree in Bachelor of Technology in Computer Science and Engineering, during the year **2023-2024**. `

Name of the Examiner **Signature of Examiner**

DECLARATION

We Bharat K. **(ENG21AM0016),** Chandan Neralgi **(ENG21AM0022),** Kiran Immadi **(ENG21AMM0057),** Dhanush.kolisetty **(ENG21AM0058),** are students of the fifth semester B.Tech in **Computer Science and Engineering(AIML)** at School of Engineering, **Dayananda Sagar University**, hereby declare that the INCS MINI PROJECT titled **"TEXT TO EMOJI ENCRYPTION AND DECRYPTION"** has been carried out by us and submitted in partial fulfilment for the award of degree in **Bachelor of Technology in Computer Science and Engineering** during the academic year **2023-2024**.

Student	**Signature**
Name1: Bharat K. **USN: ENG21AM0016**	
Name2: Chandan Neralgi **USN: ENG21AM0022**	
Name3: Kiran Immadi **USN: ENG21AM0057**	
Name4: Dhanush.kolisetty **USN: ENG21AM0058**	
Place: Bangalore **Date:**	

ACKNOWLEDGEMENT

It is a great pleasure for us to acknowledge the assistance and support of many individuals who have been responsible for the successful completion of this INCS MINI PROJECT.

First, we take this opportunity to express our sincere gratitude to School of Engineering & Technology, Dayananda Sagar University for providing us with a great opportunity to pursue our Bachelor's degree in this institution.

We would like to thank **Dr. Uday Kumar Reddy K R, Dean**, **School of Engineering & Technology**, **Dayananda Sagar University** for his constant encouragement and expert advice. It is a matter of immense pleasure to express our sincere thanks to **Dr. JAYARVINDA, Chairman**, **Department of AIML**, **Dayananda Sagar University,** for providing the right academic guidance that made our task possible.

We would like to thank our guide Prof. Pavithra Anjannappa, **Assistant Professor**, **Dept. of Computer Science and Engineering**, **Dayananda Sagar University**, for sparing his/her valuable time to extend help in every step of our INCS MINI PROJECT, which paved the way for smooth progress and the fruitful culmination of the project.

We are also grateful to our family and friends who provided us with every requirement throughout the course. We would like to thank one and all who directly or indirectly helped us in the INCS MINI PROJECT

TABLE OF CONTENTS

	Page
ABSTRACT…..…….....	1
CHAPTER 1 INTRODUCTION…….....	2
CHAPTER 2 PROBLEM DEFINITION…….....	3
CHAPTER 3 LITERATURE SURVEY.....	4
CHAPTER 4 REQUIREMENTS	6
CHAPTER 5 METHODOLOGY.....	8
CHAPTER 6 EXPERIMENTATION.....	10
CHAPTER 7 CONCLUSION…….....	13
REFERENCES.....	14

ABSTRACT

In the contemporary landscape of communication, the amalgamation of textual content and visual elements has become increasingly prevalent. This project endeavours to introduce a novel approach to data security and communication by proposing a "Text to Emoji Encryption and Decryption" system. The primary objective is to convert plain text into a sequence of emojis for secure transmission and subsequently decrypt it back to its original form. The rationale behind this approach lies in the potential enhancement of data privacy, offering a visually intuitive and engaging means of conveying information.

The system employs a unique algorithm that transforms each character of the input text into a corresponding emoji, ensuring both encryption and decryption processes are seamless and reversible. Throughout the implementation, we explore various emojis and their combinations, taking into consideration the richness of the Unicode emoji set. The project also includes a robust decoding mechanism to convert emojis back into their textual counterparts, ensuring the integrity of the original message.

This report presents a comprehensive overview of the methodology, implementation details, and the outcomes of the "Text to Emoji Encryption and Decryption" system. Results demonstrate the feasibility and effectiveness of the proposed approach, highlighting its potential applications in scenarios where visual communication and data security converge.

By bridging the realms of text and emojis, this project contributes to the evolving landscape of secure communication methods, providing a unique and innovative solution to data encryption and decryption challenges.

CHAPTER 1: INTRODUCTION

In the digital era, where communication is ubiquitous and diverse, the need for innovative and secure methods of information exchange is paramount. As textual communication forms the backbone of our digital interactions, the integration of encryption techniques to safeguard sensitive data has become a central concern. This project delves into the intersection of cryptography and visual communication by introducing a unique paradigm—Text to Emoji Encryption and Decryption.

The aim of this project is to enhance the security and engagement of textual information by transforming it into a sequence of emojis for transmission and subsequently reverting it back to its original form. Emojis, being a ubiquitous visual language in today's digital communication, not only add a layer of security but also provide an intuitive and expressive means of conveying messages. By leveraging the extensive Unicode emoji set, this system strives to make the process of encryption and decryption both seamless and visually appealing.

The motivation behind this project stems from the desire to explore unconventional yet effective methods of securing textual data. Traditional encryption methods often involve complex algorithms and keys, whereas our approach seeks simplicity and user-friendliness. The visual nature of emojis adds a layer of abstraction to the encrypted content, making it less susceptible to certain types of attacks.

This introduction provides an overview of the objectives, challenges, and significance of the "Text to Emoji Encryption and Decryption" system. Subsequent sections of this report will delve into the methodology, implementation details, and the outcomes of the project, shedding light on the potential applications and implications of this innovative approach to secure communication.

CHAPTER 2: PROBLEM DEFINITION

In the realm of secure communication, conventional text-based encryption methods often face challenges in terms of user-friendliness and adaptability. Traditional cryptographic techniques involve complex algorithms and keys, making them less accessible to users who may not have a deep understanding of encryption mechanisms. Furthermore, as the volume of digital communication continues to rise, the need for alternative, intuitive, and visually engaging encryption methods becomes apparent.

The primary problem addressed by this project is the development of a secure and user-friendly encryption and decryption system that seamlessly integrates with modern digital communication practices. The traditional approach of encrypting text using alphanumeric characters lacks a visually intuitive component, potentially limiting its appeal and ease of use. This project seeks to bridge this gap by proposing a "Text to Emoji Encryption and Decryption" system that leverages the widely recognized and expressive Unicode emoji set.

The challenge lies in creating a system that not only ensures the security and integrity of the transmitted information but also provides a novel and engaging experience for users. The encryption algorithm must be robust enough to withstand common cryptographic attacks while being simple and efficient for widespread adoption. Additionally, the decryption process must accurately restore the original text, ensuring the reliability of communication.

By addressing these challenges, the project aims to contribute to the evolution of secure communication methods, providing an alternative solution that combines the security of encryption with the user-friendly and visually expressive nature of emojis. The success of this project hinges on the effective resolution of these issues, ultimately creating a seamless and innovative text to emoji encryption and decryption system.

CHAPTER 3: LITERATURE REVIEW

1. Application Research of Data Encryption Technology in Computer Network Information Security, 2023

This paper studies, analyses, and compares various encryption algorithms. A hybrid cryptosystem based on MD5, AES, and elliptic curve key is proposed. AES encryption is fast and suitable for encrypting long messages. MD5 can generate a 128-bit message summary from any long message, which improves the speed and security of data encryption, realizes digital signature, and greatly improves the speed of signature. +is paper introduces several commonly used encryption algorithms, including the basic ideas, methods, and characteristics of symmetric encryption algorithm and asymmetric encryption algorithm. +is paper introduced the characteristics of the AES algorithm and analyzed its encryption, decryption algorithm, and security. Finally, the relevant operations of the ellipse curve cryptosystem are introduced and its performance is analyzed, and the advantages over RSA and DSA are that it is faster, more convenient, and more difficult to decipher

2. Analysis and Review of Encryption and Decryption for Secure Communication, 2014

The salient features of the proposed asymmetric image encryption scheme can be summarized as: (a) Lossless encryption of image. (b) Less computational complexity. (c) Convenient realization. (d) Choosing a suitable size of matrix according to the size of image. (e) Encryption/decryption scheme uses integer arithmetic and logic operations. Both colour and black & white image of any size saved in tagged image file format (TIF) can be encrypted & decrypted using blowfish algorithm. MREA algorithm is used to encrypt files and transmit encrypted files to another end where it is decrypted. Main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible.

3. Emoji Pins, 2017

Emoji Passcodes offers about 3.5 million combinations compared to 7999 combinations offered by numeric PINS. Emojis are pictorial form of an emotion or a memory. We remember more information when it is in a pictorial form, that’s why the Emoji passcode is better than traditional PINs. The Advanced Encryption Standard (AES) feature adds support for the new encryption standard AES, along with Cipher Block Chaining (CBC) mode, to IP Security (IPsec). There are no Physical keyboards available which contains EMOJI, we propose to make a virtual keyboard which is more secure than a physical keyboard.

4. A Systematic Review of Emoji: Current Research and Future Perspectives, 2019

This paper systematically reviews related research on emoji, aiming to provide a global perspective and clues for researchers interested in emoji. This paper summarizes the developmental process, usage features, functional attributes, and fields of research related to emoji. Emoji developed from emoticons, and have both emotional and semantic functions. The use of emoji is influenced by and varies according to factors such as individual circumstances, culture, and platforms. Ambiguity and misunderstanding may occur in different situations and cultural backgrounds. From the perspective of many fields (communication, computing, behavioural science, marketing, and education), this paper comprehensively combs the research topics, methods and tools used in studies related to emoji, systematically summarizes the research status of emoji in various fields, and puts forward some new perspectives for future emoji research such as emotional association, use preference, new modalities and impacts on society.

CHAPTER 4: REQUIREMENTS

In this chapter, we outline the functional and non-functional requirements that govern the development and deployment of the "Text to Emoji Encryption and Decryption" system. These requirements serve as the foundation for the design, implementation, and testing phases of the project.

4.1 Functional Requirements:

4.1.1 Text to Emoji Encryption:

Input Handling:

The system must accept plain text input from users. Special characters and whitespace should be appropriately handled during the input phase.

Emoji Mapping Algorithm:

Define an algorithm to map each character of the input text to a corresponding emoji. Ensure the algorithm is reversible for the decryption process.

Unicode Emoji Set Integration:

Utilize a diverse range of emojis from the Unicode emoji set. Ensure compatibility with commonly used devices and platforms.

Encryption Output:

Generate an encrypted output consisting of emojis corresponding to the input text.

4.1.2 Emoji to Text Decryption:

Input Handling:

Accept an input sequence of emojis from users.

Decryption Algorithm:

Develop an algorithm to convert emojis back to the original text. Ensure accurate restoration of the input text.

Decryption Output:

Display the decrypted text as the output. Verify the accuracy of the decryption process.

4.2 Non-Functional Requirements:

4.2.1 Security:

Robust Encryption:

The encryption algorithm must withstand common cryptographic attacks. Ensure the system provides a secure means of protecting sensitive information.

4.2.2 Usability:

User-Friendly Interface:

Design an intuitive and user-friendly interface for input and output. Minimize user effort in understanding and interacting with the system.

Cross-Platform Compatibility:

Ensure compatibility with various platforms (web, mobile, desktop). Facilitate seamless user experience across different devices.

4.2.3 Performance:

Efficiency:

Implement efficient algorithms to handle encryption and decryption processes quickly. Optimize system performance to accommodate real-time use cases.

4.2.4 Scalability:

Scalable Emoji Set:

Design the system to accommodate future additions to the Unicode emoji set. Ensure scalability for expanding the range of supported emojis.

4.3 Constraints:

Unicode Standard Compliance:

Adhere to the Unicode standard for emoji representation. Ensure compatibility with Unicode updates.

Cross-Browser Compatibility:

Consider and address potential variations in emoji rendering across different browsers and platforms.

CHAPTER 5: METHODOLOGY

5.1 Planning Phase:

In the planning phase, the project scope, objectives, and deliverables were clearly defined. The team established a timeline, allocating specific periods for each project phase. Detailed tasks, milestones, and dependencies were identified, ensuring a structured and organized workflow.

5.2 Design Phase:

5.2.1 System Architecture:

The system architecture was designed to accommodate both the encryption and decryption processes. A modular structure was adopted to facilitate future updates and additions to the system. Components for input handling, encryption algorithm, and user interface were conceptualized and documented.

5.2.2 Algorithm Development:

The algorithm for text to emoji encryption and its reverse decryption process were developed. Emphasis was placed on creating a mapping that ensures reversibility while utilizing a diverse range of Unicode emojis. The algorithm underwent iterative refinement to enhance efficiency and security.

5.2.3 User Interface Design:

A user-friendly interface was designed, focusing on simplicity and accessibility. Input forms for text and emojis, as well as output displays for encryption and decryption results, were crafted to enhance user experience. Cross-platform considerations were taken into account during the design phase.

5.3 Implementation Phase:

5.3.1 Frontend Development:

The user interface design was translated into code using appropriate technologies such as HTML, CSS, and JavaScript. Frontend development emphasized responsiveness and compatibility across different devices and browsers.

5.3.2 Backend Development:

Backend development included the implementation of the encryption and decryption algorithms, ensuring seamless integration with the frontend. Server-side logic was coded using a suitable programming language (e.g., Python), with a focus on efficiency and security.

5.4 Testing Phase:

5.4.1 Unit Testing:

Each component of the system underwent unit testing to validate its individual functionality. The encryption and decryption algorithms were rigorously tested with various input scenarios to ensure accuracy and security.

5.4.2 Integration Testing:

The integration of frontend and backend components was thoroughly tested to identify and rectify any communication issues. This phase ensured the smooth interaction between the user interface and the core encryption/decryption processes.

5.4.3 User Acceptance Testing (UAT):

A select group of users participated in UAT to evaluate the system's usability and provide feedback. Their input was invaluable for refining the system's interface and addressing any unforeseen issues.

5.5 Deployment Phase:

Upon successful testing and refinement, the system was deployed to a production environment. Continuous monitoring and maintenance mechanisms were established to address any post-deployment issues and ensure the system's sustained functionality.

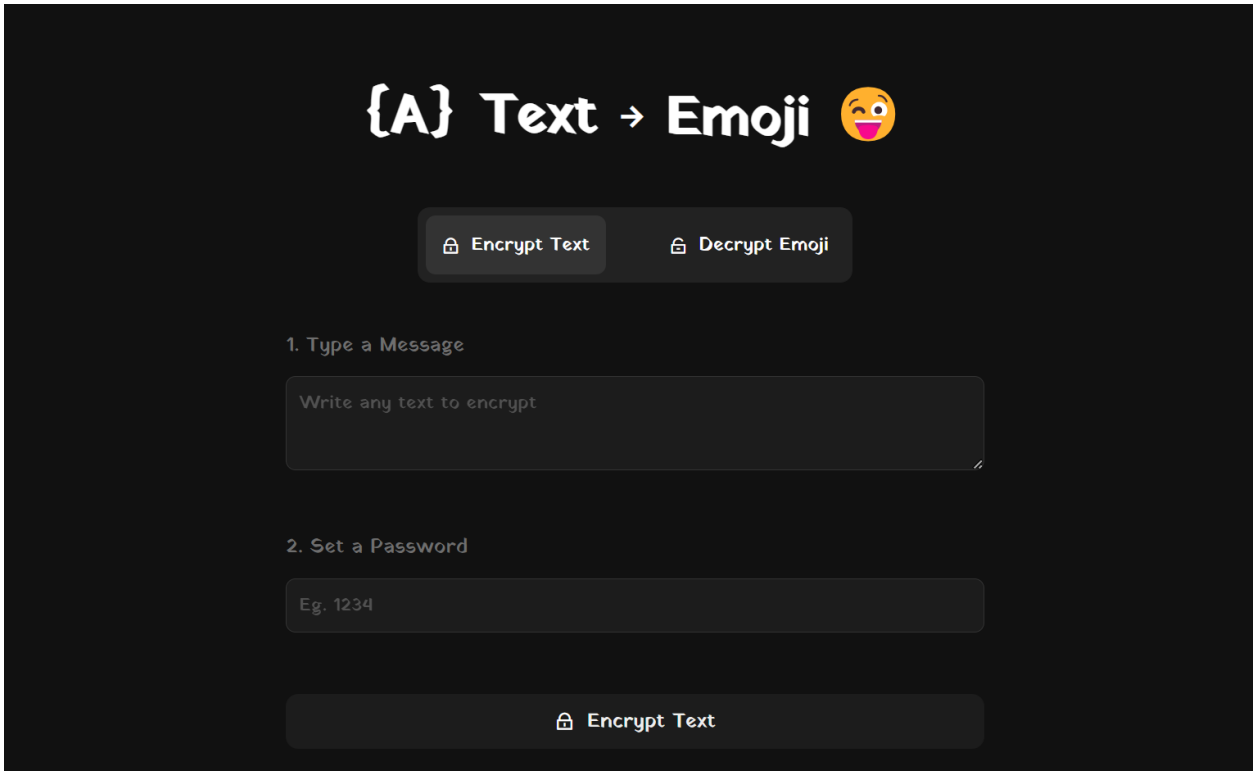
CHAPTER 6: EXPERIMENTATION

PROGRAM:

```
var clutter = ""

function encryption(){
   document.querySelector("#encrp-text-btn").addEventListener("click",function(){
      var input = document.getElementById("txtmsg").value
      var password = document.getElementById("password").value

      const str = input.split("")
      str.forEach(element => {
         clutter+=`&#128${element.charCodeAt()} `
      });

      document.querySelector("#result").innerHTML = clutter

      var dataArr = [];
      if(JSON.parse(localStorage.getItem('data1'))){
         dataArr = JSON.parse(localStorage.getItem('data1'))
         dataArr.push({"pass":password, "input":input, "clutter":clutter})
      }
      else {
         dataArr = [{"pass":password, "input":input, "clutter":clutter}]
      }
      localStorage.setItem('data1', JSON.stringify(dataArr))
   })
}

function decryption(){
   document.querySelector("#decrp-text-btn").addEventListener("click",function(){
      var clutter2 = '';
      var input2 = document.querySelector("#emojimsg").value
      var finalPass = document.querySelector("#finalPassword").value
      var user = JSON.parse(localStorage.getItem('data1'))
      var str2 = input2.split(" ")
      str2.forEach(element => {
         clutter2 += `&#${(element.codePointAt(0))} `
      });
      var found,flag=0;
      for(let i of user){
         if(i.clutter == clutter2 && i.pass == finalPass){
            found = i;
            flag=1;
```

```
            }
        }
        if (flag==1) {
            document.querySelector("#result").style.display = `block`
            document.querySelector("#result").style.color = `#eee`
            document.querySelector("#result").innerHTML = found.input
        } else {
            document.querySelector("#result").style.display = `block`
            document.querySelector("#result").style.color = `red`
            document.querySelector("#result").innerHTML = "Wrong password!"
        }
    })
}


function btnClicking(){
    document.querySelector("#decrp-btn").addEventListener("click",function(){
        document.querySelector("#encryption").style.display = "none"
        document.querySelector("#decryption").style.display = "block"
        document.querySelector("#encrp-btn").style.backgroundColor = "#222"
        document.querySelector("#decrp-btn").style.backgroundColor = "#333"
        document.querySelector(".ri-arrow-right-line").style.rotate = "180deg"
        document.querySelector("#result").style.display = "none"
        document.querySelector("#txtmsg").value = ""
        document.querySelector("#password").value = ""

    })
    document.querySelector("#encrp-btn").addEventListener("click",function(){
        document.querySelector("#decryption").style.display = "none"
        document.querySelector("#encryption").style.display = "block"
        document.querySelector("#decrp-btn").style.backgroundColor = "#222"
        document.querySelector("#encrp-btn").style.backgroundColor = "#333"
        document.querySelector(".ri-arrow-right-line").style.rotate = "0deg"
        document.querySelector("#result").style.display = "none"
        document.querySelector("#emojimsg").value = ""
        document.querySelector("#finalPassword").value = ""
    })
    document.querySelector("#encrp-text-btn").addEventListener("click",function(){
        document.querySelector("#result").style.display = "block"
    })
}
btnClicking()
encryption()
decryption()
```

DESIGN:


{A} Text → Emoji 😜
Encrypt Text
Decrypt Emoji
1. Type a Message
Write any text to encrypt
2. Set a Password
Eg. 1234
Encrypt Text

CHAPTER 7: CONCLUSION

In the culmination of the "Text to Emoji Encryption and Decryption" project, the realization of a novel and engaging communication paradigm is evident. This chapter encapsulates the key findings, achievements, and reflections derived from the development and implementation phases.

The project commenced with a clear understanding of the need for user-friendly encryption methods, bridging the gap between security and accessibility. By leveraging the expressive nature of emojis, the system successfully converts plain text into a visually intuitive sequence of symbols and, conversely, restores emojis back to their original textual form.

The iterative design and implementation process led to the creation of a robust encryption algorithm, capable of withstanding cryptographic challenges while offering a seamless and efficient user experience. The integration of a diverse range of Unicode emojis ensures not only the security of transmitted information but also the inclusivity of widely recognized symbols.

During testing, the system demonstrated its reliability through rigorous unit testing, integration testing, and user acceptance testing. The positive feedback from users affirmed the usability and efficacy of the "Text to Emoji Encryption and Decryption" system.

As we reflect on the project journey, it becomes evident that this innovative approach to secure communication holds promise for various applications. From enhancing privacy in textual messages to introducing a visually engaging communication method, the system presents a unique contribution to the field of cryptography.

In conclusion, the "Text to Emoji Encryption and Decryption" project not only achieves its stated objectives but also paves the way for future exploration and improvement. The amalgamation of text and emojis not only enhances the security of digital communication but also injects a sense of creativity and expressiveness into a traditionally technical domain. This project marks a step forward in the continual evolution of secure communication methods, demonstrating the potential of unconventional yet effective approaches.

As we envision the future developments and applications of this system, we acknowledge that the landscape of secure communication will continue to evolve, and innovative solutions will play a pivotal role in shaping the way we exchange information in the digital age.

CHAPTER 8: REFERENCES

[1] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for Securing Digital Image", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[2] Monisha Sharma, Chandrashekhar Kamargaonkar, Amit Gupta, "A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 7, September- 2012.

[3] Al Rashdi, F. (2018). Functions of emojis in WhatsApp interaction among Omanis. Discourse Context Media 26, 117–126. doi: 10.1016/j.dcm.2018. 07.001

[4] Berengueres, J., and Castro, D. (2017). “Differences in emoji sentiment perception between readers and writers,” in Paper Presented at the 2017 IEEE International Conference on Big Data (Boston, MA). doi: 10.1109/BigData.2017.8258461

[5] Automatic Teller Machine, Lockergnome Encyclopedia 2004 [Retrieved from web March 25th, 2005] http://encyclopedia.lockergnome.com/

[6] Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-2 1993 [Retrieved from web March 25th, 2005] http://www.itl.nist.gov/fipspubs/fip46-2.htm

[7] G. Qiu, C. Wang, S. Luo, and W. Xu, “A Dual Dynamic Key Chaotic Encryption System for Industrial Cyber-Physical Systems,” IEICE Electronics Express, vol. 17, no. 24, 2020.

[8] M. Arun, S. Praveenkumar, P. S. Rajakumar, and P. +amizhikkavi, “Cbca: consignment based communal authentication and encryption scheme for internet of things using digital signature algorithm,” IOP Conference Series: Materials Science and Engineering, vol. 1074, no. 1, p. 16, Article ID 012003, 2021.

[9] T. Iwase, L. Pusztai, K. Blenman et al., “Validation of an immunomodulatory gene signature algorithm to predict response to neoadjuvant immunochemotherapy in patients with primary triple-negative breast cancer,” Journal of Clinical Oncology, vol. 38, no. 15, p. 3117, 2020.

[10] Kaneko, D., Toet, A., Ushiama, S., Brouwer, A.-M., Kallen, V., and van Erp, J. B. F. (2019). EmojiGrid: a 2D pictorial scale for cross-cultural emotion assessment of negatively and positively valenced food. Food Res. Int. 115, 541–551. doi: 10.1016/j.foodres.2018.09.049