International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

A STRONG AND PRACTICAL AUTHENTICATION MECHANISM USING PASSTEXT AND ONE MINUTE PASSCODE

[1] Ramya M R, [2] Abijith U, [3] Charan K, [4] Nalini V, [5] Shibivarsan J
[1]Assistant Professor, Department of Information Technology, Nandha College of Technology, Erode-638 052
[2,3,4,5] UG-Final year, Department of Information Technology, Nandha College of Technology,Erode-638 052
[1] ramyamanidhiva@gmail.com ,[2] abiabijitj@gmail.com, [3] charankathirvel17@gmail.com ,[4] nalini.v2003@gmail.com , [5]varsanshibi@gmail.com

----------***----------

ABSTRACT

In this modern world, hacking is growing faster, and there is no privacy for personal data. Therefore, we have decided to create passwords using new methods. This project demonstrates that there is no secret shared between the user and strangers; it presents a one minute challenge to unlock private data. Our project generates random codes minute by minute, and each password is only valid for just one minute, which is called OMP (One Minute Passcode). Therefore, the user doesn't know the correct password at all times. These passkeys are then sent to the user's mobile phone using the Twilio method, which is more secure and provided by Google to communicate through secret authentication methods and tokens. Thus, hacking becomes impossible with this level of complexity. In the future, if there's a possibility of hacking, we will update the cipher methods to unlock the data. Nowadays, the usage of PCs and mobile phones has increased rapidly. What if the passwords are not known by the user or strangers in this modern technology. Our project ensures privacy between users and hackers or strangers; secret passwords may sometimes be compromised, but random passwords will never be known to users or strangers. This idea is used here to maintain safety while unlocking our privacy or private sectors by creating random codes and sending them to the user's mobile IP value or number. We can easily unlock our device in a non-hackable form using brute force and Twilio, which are the main components of our data protection system. In the older authentication method, there were only 6-digit numbersto unlock data, which were available only for apps. Like an OTP, this method randomly generates a 6-digit code to unlock the private sector, which is available on the same phone or PC. This makes it easy for hackers to access details using your phone number or email. These passkeys are dynamic and not stable at all times, and theirsize istoo small. A relational database plays a major role here, we also use the emergency password method for user convenience.

KEYWORDS: *Security Authentication, Twilio, Database, Spyware attacks, Hacking, Password Authentication,Database.*

I. INTRODUCTION

Nowadays, the usage of PCs and mobile phones has increased rapidly. What if the user forgets their passwords or if a stranger attempts to hack into these modern technologies.Our project addresses this concern by implementing a new password method that generates random passkeys every minute. With this feature, users can unlock their private sectors, PCs, mobile apps, and even bank lockers to prevent data theft and hacking.Our project ensures privacy between the user and potential hackers or strangers. While traditional passwords may be

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

compromised at times, random passwords generated by our system remain unknown to both users and strangers, enhancing security. These random codes are sent to the user's mobile IP value or number, allowing easy and secure unlocking of devices.Brute force and Twilio are key components in protecting our data and securing us from hacking attempts. Unlike older authentication methods that rely on easily hackable 6-digit codes, our system generates dynamic passkeys that are not stable and are of a larger size, making them harder to crack[1].In the past three years, this method has been implemented primarily for apps and emails to safeguard data, yet only 25% of people have adopted it. Similar to OTPs, our method generates random 6-digit codes to unlock private sectors, but it is more secure as it creates unique codes that change every minute, making it difficult for hackers to predict or an make a intercept.Authentication serves to increase security and add capabilities dynamically without compromising data integrity. Our project focuses on addressing privacy and security issues for PCs, bank lockers, and other sensitive data repositories, employing techniques to ensure non-hackable password management databases. Our methodology involves using random passkeys where each incoming request is redirected transparently to the user, generating a code valid for only one minute before changing randomly. Brute force attacks are effectively mitigated, ensuring password strength remains static and sequential without repetition once a code appears.Invalid password entries trigger audible alarms. Python code is utilized for password generation and storage management within a relational database. Twilio, provided by Google, further enhances security by preventing hacking attempts. Figure 1.1 illustrates the passwords received to an user/client mobile phones. Our project ensures privacy between users and hackers or strangers; secret passwords may sometimes be compromised, but random passwords will never be known to users or strangers. This idea is used here to maintain safety while unlocking our privacy or private sectors by creating random codes and sending them to the user's mobile IP value or number. We can easily unlock our device in a non-hackable form using brute force and Twilio, which are the main components of our data protectionsystem. In the older authentication method, there were only 6-digit numbersto unlock data, which wereavailable only for apps. However, this method was not strong and was easily hacked using brute force attacks and hashing techniques. Over the past 3 years, this process has been implemented only for apps and emails to safeguard their data, but it hasn't been widely adopted by users worldwide; only 25% of people have used this method. Like an OTP, this method randomly generates a 6-digit code to unlock the private sector, which is available on the same phone or PC. This makes it easy for hackers to access details using your phone number or email. These passkeys are dynamic and notstable at all times, and theirsize istoo small. A relational database plays a major role here, we also use the emergency password method for user convenience.

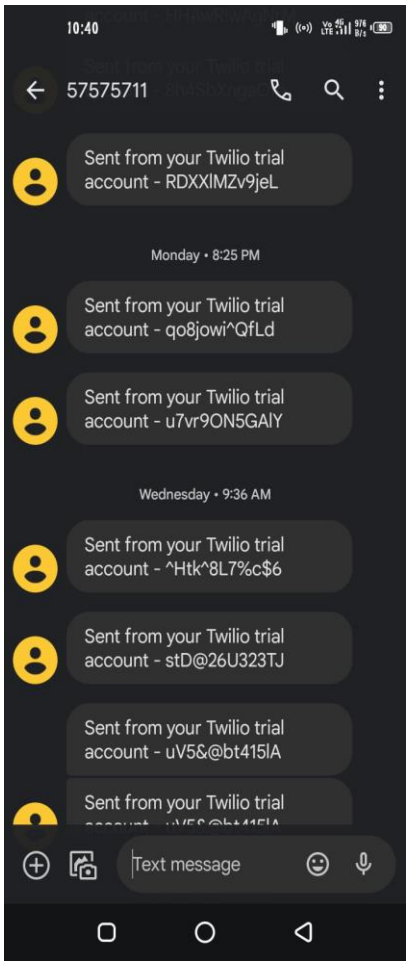


Fig.1.1 Passwords received to user phone

II.TWILIO ACCOUNT VERIFICATION

Twilio is a platform that provides a separate number to users for their personal use to send and receive messages from one entity to another. This platform is used to check major passkeys, and upon logging in, it provides separate authentication and tokens for individual users. With this, users can send up to 500 messages from their account. This technology assists in generating random passkeys with a length of 12 characters, mixing lowercase and uppercase letters. This method ensures secure

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

authentication mechanisms. We hope to use this website instead of others, as all other websites typically require payment. [2] This platform's account is utilized in server-side scripting within Visual Studio Code using JavaScript code with the help of Node.js and Twilio's server. We can generate random passkeys within a sector of our project using Twilio's server.

The generated passkeys are controlled by a relational database that stores them securely, ensuring they are not generated again and are stored correctly. These passkeys are strong and serve both the "send" button and the "emergency" button. The emergency button generates a 4-digit password, while the send button generates a 12-digit password, both of which are highly secure. This method functions similarly to OTP (One-Time Password), but our project implements OMP (One Minute Passcode), changing the passcode every minute. This approach makes hacking virtually impossible, as even if a hacker attempts to breach the system, the user authentication process remains secure and protects the data. Brute force algorithms and SHA algorithms play a significant role in safeguarding the data. The use of blockchain technology is not applicable in this context.

Fig 2.1 depicts the relational database utilized in this project to store the generated passwords and random keys. This method ensures that stored passkeys cannot be repeated, thus enhancing security significantly [3]. The 12-digit random keys are generated using a random code and executed in the background, interfacing with the database. The server method ensures that stored data is kept and maintained securely, making it impervious to hacking attempts.

	A	B	C
17	JYvyJ6f0	pp1zvjyV	G9XGBFQJ
18	ngSk8AdW	pUnH34hi	GN2xBbYD
19	sfTGpWbE	HlKnn51p	MfJa6qcL
20	cy9yMcIL	HP2dqWqS	3i9Ru34L
21	VNlfR7HB	DIo0Wm1p	d9fXDY9z
22	z0gXqKbi	4yc90n3K	I0Zhsz6Q

Fig 2.1 Relational database of Password

2.1.Password analysis and generation:

Using Python, random passwords are created with a length of 12 characters. This code is then converted into JavaScript and linked with Twilio tokens and authentication methods to receive messages from one phone number to another. These passwords consist of strong letters and are not easy to spell or remember[4]. The time complexity is low, so random passwords are generated minute by minute to ensure they are never repeated.The generated passwords are stored in a relational database to check if the passwords are equal or not. If the same password is detected, it is discarded, and another password is generated. Passkeys are unique and sent to the user when they click the "send" button on the login page.After receiving the passkey, the user can view the code and enter it on the portal or input the correct PIN to unlock the database. The user needs to enter their username and press the "send" button to receive the passkeys on their phone. These passkeys are a mix of lowercase and uppercase letters, as well as special characters. This is the basic process for entering the password, and if not done correctly, the user cannot log in. Twilio sends the random code to the user's mobile through a message or WhatsApp.

III. PROBLEM DOMAIN

Authentication is a means to enhance security or dynamically add capabilities without compromising data integrity or making other modifications. This project specifically addresses privacy and security concerns related to PCs or bank lockers, employing techniques to create a non-hackable password management database. OMP (One Minute Passcode) is implemented using random passkeys, where each incoming request is transparently redirected. The passkey is valid for only one minute before being randomly changed [5]. Proper maintenance against brute force attacks is ensured. The system is static, consistently generating strong passwords in a sequential manner, and passwords are never repeated once they have been used.

3.1.Proposed Solution

This authentication method is designed to generate strong passwords randomly to unlock private data on PC lock screens, phone apps, and bank lockers. Invalid password entries trigger an audible alarm. Python code is utilized to generate passwords and store them in a

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

specific relational database. Password storage management plays a crucial role in this process. The use of Twilio, provided by Google, adds an extra layer of security to prevent hacking in this project.

3.1.2.Algorithm for the proposed solution:

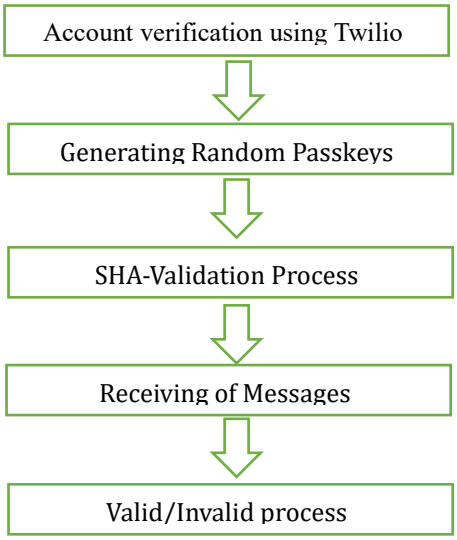
- SHA- ALGORITHMS.
- HA-ALGORITHMS.
- BRUTE FORCE ATTACK.
- CIPHER TEXT (algorithm if need).

```
Algorithm 1 Login Procedure at Server
Input : OTP as an array of 4 elements
Output: Grant access or wrong password
Initialize: otp_server = [], X = 0;
for i = 0 to 3 do
otp_server[i] = (P[i] + R[i]) mod 10;
end
for j = 0 to 3 do
if otp_server[j] = OTP[j] then
X ← 1;
else
X ← 0;
break;
end
end if X == 1 then grant access;
else
   wrong password;
end
```

Fig 3.1 Algorithm for the OMP/OTP Generation

Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to secure data. The SHA algorithm plays a major role in our project. The secure methods are set to safeguard data within this unit, and the SHA method is used to retrieve stored data efficiently, aiding in data maintenance. The SHA validation process is unique [6], preventing repetition within this unit and protecting data from potential hacking attempts. This method is superior compared to others because it establishes a unique database for storing data securely. Therefore, it is considered superior to other methods and is the most widely used algorithm in recent times.

3.2 FLOWCHART



3.2. Flowchart for the Proposed Algorithm

IV. SECURITY ANALYSIS

1) Security analysis is essential for ensuring the security of our methods, particularly in the manner akin to OTP (One-Time Password), which we've transformed into a one-minute passcode system. This approach has been widely adopted in recent times to secure data effectively. The 12-digit random code and the randomly generated 4-digit emergency code are collected and processed to strengthen the algorithm, ensuring data safety. These lengths are commonly employed to enhance data security. Python code is used to generate random passcodes, preserving user privacy and minimizing the risk of hacking. However, user convenience is also paramount, which is why we've opted for 4-digit passcodes [7]. This decision improves user experience while maintaining data security. Additionally, our security analysis incorporates an alarm system to alert us of any attempts to breach data security, thereby thwarting hacking attempts effectively and

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

securely. Fig 4.1 illustrates the Twilio verification method. Twilio is a secure platform that allows users to send messages through various platforms such as WhatsApp, Gmail, normal text messages, or Instagram. These platforms offer different means of communication to describe this process. These platforms include five methods to pass the random passkeys to access the account and activate it by providing tokens and authentication.

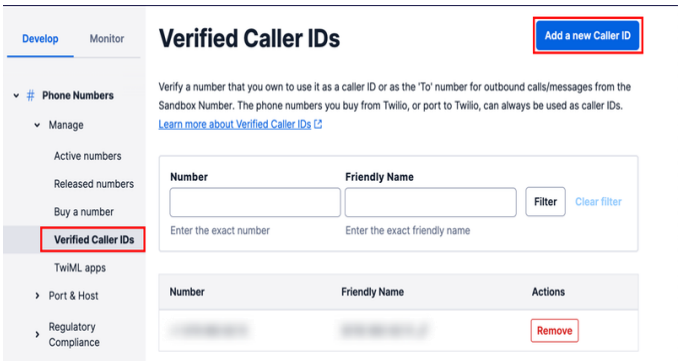


Fig 4.1 Twilio account verification

2) Normally, an OTP is a method that generates a 6-digit or 4-digit code as a random passkey, which is sent to a user's phone. The system checks if the entered OTP matches the one generated, allowing login if correct. OTPs are typically valid for 10 to 30 minutes. However, our project generates random codes of 12 digits, valid for only 1 minute before being replaced with another password. These passwords are stored in a relational database and are not repeated, minimizing hacking risks. This method is commonly used for PC logins, bank lockers, and app locks, providing heightened security. We can further enhance security by increasing the length of the code beyond 12 digits or making it 30 digits long. Trust in this method is crucial, even though shorter codes like 6 or 4 digits are more common, as our project prioritizes higher security. Fig 4.2 describes the types of security through a public perspective in different years. This method incorporates an authentication process, which is crucial in our efforts to maintain data security. Nowadays, there is a growing emphasis on safeguarding data, making this method suitable for various applications. The minute-by-minute password change ensures that privacy is not compromised, and we can confidently assert that we are ensuring 100% data safety. The SHA algorithm is extensively employed to ensure data safety, resulting in more losses for hackers attempting to breach it due to the one-minute challenge, which proves exceedingly difficult and little bit hard.

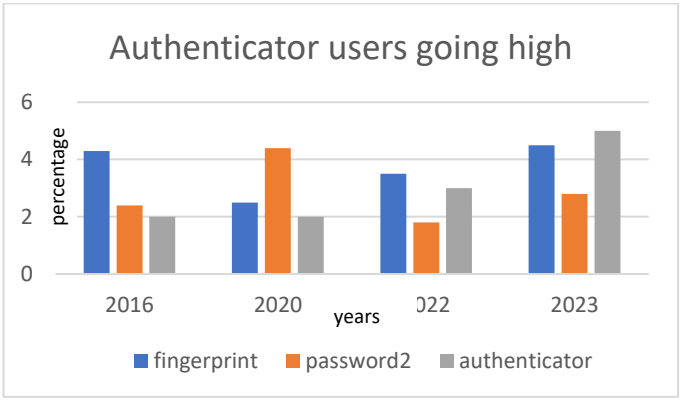


Fig 4.2 Comparision Graph

Similar to the OTP PIN entering system, this method also requires entering a PIN. However, in this approach, instead of using a traditional PIN, users input a 12-digit random passkey or a 4-digit emergency PIN to access the login page, ensuring high security. Actually, this PIN entry system is entirely unique. Users must input the correct PIN without error; otherwise, the security alarm will trigger. This method ensures data safety by swiftly detecting and responding to hacking attempts.

3) Normally, the OTP PIN is shared with the user, but this method prohibits forwarding the message to user details. Therefore, user details are not stored in a relational database to safeguard the random passkeys, which are stored using the SHA algorithm. These security measures, coupled with server scripts, utilize the Twilio method to secure data. The most valuable random passkeys are involved in this process, necessitating thorough code checks using Twilio modules and separate [8] code provided by the Twilio server. The Twilio method provides a separate Node.js module and NPM to start the code. When the server begins running, it retrieves the code and generates the correct random code keys, subsequently verifying them in the correct order. PIN secure methods are highly utilized to ensure the correctness of the code, thereby generating random passkeys without allowing repetition. The brute force algorithm is employed to maintain data integrity, making this method inherently safe and resistant to user hacking attempts. The validation process, distinguishing between valid and invalid inputs, plays a pivotal role. Additionally, the localhost method and the Figma tool are employed to design the user interface, while JavaScript and server

ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

methods are utilized for fetching data, serving as the primary methods in this process.

4) In traditional systems, such as PCs, users typically have static passwords that remain unchanged until manually updated. However, in our project, this approach is entirely transformed. We employ random passkeys that dynamically change every minute, ensuring enhanced security. The fetch method is particularly secure, facilitating secure communication between the server and JavaScript. Access is denied by the local server host, adding an extra layer of security. Overall, the system is fully secured through JavaScript and server communication. The fetch method [9], a key component in our system, ensures secure communication between the server and JavaScript. It facilitates the exchange of data in a manner that is robust and resistant to potential breaches.Moreover, access control is fortified through denial by the local server host. This means that unauthorized attempts to access the system are met with resistance at the server level, adding an extra layer of protection against potential threats.The entire system architecture is meticulously designed to prioritize security. JavaScript and server communication form the backbone of our security infrastructure, ensuring that data transmission and interaction processes are safeguarded at every step. The codes are tailored to be highly secure, and the PINs are equally robust [13], making it challenging for hackers to succeed. With the rapid advancement of AI and ML technologies, potential threats may emerge in the future. However, our project is continuously evolving to stay ahead of these challenges. We employ cutting-edge technologies to enhance data protection [11] and thwart attackers. Thus, our method remains highly secure until new technologies are developed. The robustness of our codes and the strength of our PINs pose significant challenges for potential hackers. As AI and ML technologies continue to advance at a rapid pace, there is a possibility that new methods for breaching security may emerge in the future. However, our project is committed to staying ahead of these potential threats by continuously enhancing our security measures.

5) We leverage the latest advancements in technology to bolster data protection and safeguard against attacks. By staying proactive and vigilant, we ensure that our methods [12] remain highly secure. While no system is entirely immune to hacking, our approach significantly mitigates the risk and makes it exceedingly difficult for attackers to compromise our data.As we continue to evolve and adapt to emerging threats, we remain confident that our security measures will remain effective in safeguarding our data. Our commitment to staying at the forefront of security technology ensures that we can address any new challenges that may arise in the future.

4.1 PIN-ENTRY TIME AND ALARM

In this module, if an incorrect PIN is entered into the login sector, the alarm or beep sound will start alarming. When the correct PIN is entered, the interface will open. However, if an incorrect PIN is entered, the alarm will continue until the user corrects the PIN [10]. This helps identify hackers and secure the data from theft. The correct PIN, delivered to the user's phone, can be entered to access the interface and safely store data on the PC or in lockers. The length is checked, and there is an emergency button available on this page for user convenience. The emergency button functions as a cipher method; when clicked, a 4-digit alphabet is sent to the user's phone. Instead of entering the generated code directly, the user enters a code that shifts each letter by three digits. For example, A becomes D, B becomes E, and so on. This is the major method we use here for user convenience and fast access to the login page sector to safeguard data from hackers or theft attempts.

V. ACKNOWLEDGEMENT

We aim to highlight this project for high-level security management by transmitting passwords through users' mobile phones. This method ensures an un hackable code, making it impossible to crac4k the password within a minute, as it changes randomly. In the future, this technology will continue to advance, and new technologies will emerge.

VI. CONCLUSION

In this project we done the security protection in an high range and make the non hackable form of code by using twilio methods.This technology was not in process still now after this we plan to publish this techniques to secure the data on whole world .In this modern technology the hacking is growing day by day ,Our project may also been hacked in future there has a possibility to hack but we try our best to protect the data using modern.Technology, May be in future we also develop this project in high security using advanced technologies.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01671

REFERENCES

[1]. Ashbourn, J., 2014. Biometrics: Advanced Identity Verification: The Complete Guide. 1st Edn., Springer, Berlin, Germany, ISBN-10: 1447107470, pp: 200.

[2]. Ashfield, J.M., 2016. Method for using at least a portion of a one-time password as a dynamic card verification value. U.S. Patent 9,251,637 [current assignee: Bank of America Corp].

[3]. M. Karthick, Dinesh Jackson Samuel, B. Prakash, P. Sathyaprakash, Nandhini Daruvuri, Mohammed Hasan Ali, R.S. Aiswarya, Real-time MRI lungs images revealing using Hybrid feed forward Deep Neural Network and Convolutional Neural Network, Intelligent Data Analysis 27 (2023) S95–S114, DOI 10.3233/IDA-237436

[4]. Browne, S., 2010. Digital epidermalization: Race, identity and biometrics. Critical Sociol., 36: 131-150.DOI: 10.1177/0896920509347144Cashell, B., W.D. Jackson, M. Jickling and B. Webel,

[5]. CRS RL32331. Congressional Research Service, Library of Congress, Washington, USA.Centeno, C., R. Van Bavel and J.C. Burgelman, 2005. A prospective view of e-government in the European Union.

[6]. S.Satheesh Kumar, M.Karthick, An Secured Data Transmission in MANET Networks with Optimizing Link State Routing Protocol Using ACO-CBRP Protocols, IEEE Access, 2018.

[7]. Cisco, San Jose, USA.Della Penna, G., P. Frasca and B. Intrigila, 2019. Two factor authentication for e-government services using hardware-like one time password generators. J. Comput. Sci., 15: 171-189.DOI: 10.3844/jcssp.2019.171.189Dmitrienko, A., C. Liebchen, C. Rossow and A.R. Sadeghi, 2014. Security analysis of mobile two-factor authentication schemes.

[8]. European Commission, Brussels, Belgium.Hashizume, K., D.G. Rosado, E. Fernández-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Services Application.

[9]. Intel OTP J., 18: 138-161.European Commission, 2018. Annex to the commission implementing decision: Laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by member states and repealing decisions C(2006) 2909 and C(2008) 8657.

[10]. Hashizume, K., D.G. Rosado, E. Fernández-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Services Application. .

[11]. Bremananth, R. and A. Chitra, 2006. New methodology for a person identification system. Sadhana, 31: 259-276. DOI: 10.1007/BF02703381

[12].]. CNMJ RL32331. Congressional Research Service, Library of Congress, Washington, USA.Centeno, C., R. Van Bavel and J.C. Burgelman, 2005. A prospective view of e-government in the European Union.

[13]. Karthick.M, Salomi Samsudeen, Likewin Thomas, Priya Darsini.V, Prabaakaran.K, Cybersecurity Warning System Using Diluted Convolutional Neural Network Framework for IOT Attack Prevention, International Journal of Intelligent Engineering and Systems, Vol.17, No.1, 2024, DOI: 10.22266/ijies2024.0229.66