*Nanotechnology Perceptions*
*ISSN 1660-6795*
*www.nano-ntp.com*

# Factorizing Analysis of Two Factor Authentication Techniques for Rapid and Secure Communication

**S. Ragunathan[1], A. Krishnaveni[2]**

*[1]Ph.D., Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Deemed to be University Coimbatore, India*
*[2]Assistant Professor, Department of Computer Science, Karpagam Academy of Higher Education, Deemed to be University Coimbatore, India*
*Email: ragu34salem@gmail.com*

Rapid and secured communication through network has various challenges in the entire communication environment. Internet of Things (IoT) has different applications which will be considered for user friendly access and improved security. Biometric identification of user through iris, fingerprint, etc., is broadly accessed for data processing to identify the user detail through authentication approach. To enhance the security of user data while communication two factor authentication which will integrate the user identification data including token and device information to enhance the authentication of security level. In this study paper, a brief scheme of two factor authentication system for intelligent communication by proposing the watermarking technique for incorporating the authentication of data for user data in validation model. The proposed study provide the user friendly environment to improve the security of user and reduce the authenticity of data sharing procedures with lightweight model and security measures in real world applications. The merits of schema to validate the security using automated validation of internet with security protocols and application, and the execution of the study will showcase the innovation methods for protecting the data with enhanced security model for rapid communications between the users.

**Keywords:** Two factor methods, Watermarking, Cyber security, Authentication.

## 1. Introduction

In a developing technology the number of communication devices connected to internet has growing faster and different type of applications from various industries like commercial, industrial, personal applications, etc., are deployed mechanisms of Internet of Things, which

will run their smart devices to maintain the record of their day to day life for protecting from the unauthorized access through IoT devices to IoT systems from security threats. The smart intelligent technologies are proposed for the user convenience to share the data between two devices and there should be a communication gateway for allowing the network to be affected by the attacks over insecure communication links which will leads to cyber attacks, data modification, etc., Secure authentication is the important factor which should be prioritized for the development of higher security level. The scheme known as conventional authentication were designed to explore the authentication of security factor with information about the identity of user. Now a day, a modern two factor authentication system is explored for the preserving process of user data from smart access such as fingerprint scans, iris recognition, etc., to enhance the security level for better performance, convenience, and deployment of the application with developers. The two factor authentication scheme is considered as an end user identity for enhancing the security level to improve the protection of data which has the demerit has user cannot hike the work load integrated with processing the sensitive data. Few smart applications have only limited processing capacity which is also a strong to the human activity for developing the user friendly procedures. To prioritize the convenience of smart applications we perform the one to one mechanism for establishing the two factor authentication model to combine the smart process of data accessing in the smart devices for identification.

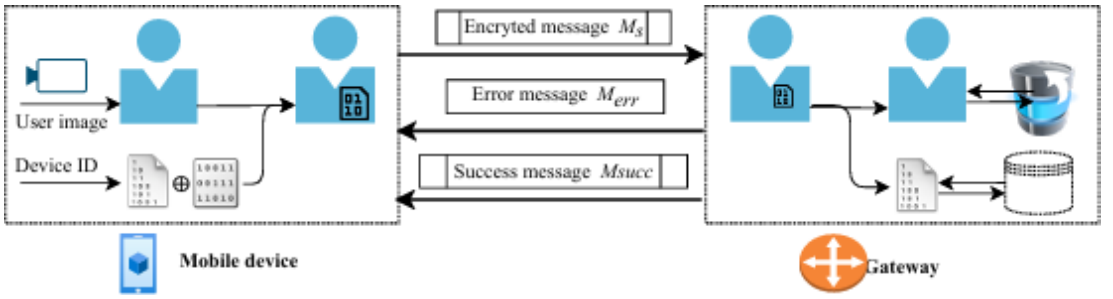


Figure 1: Process of two factor authentication model.

The proposed study targeted to increase the security level for better and secure communication using integrated authentication system with watermarking techniques. The major contribution is categorized as, multi factor authentication scheme based on data recognition for user convenience and secure data access. It used to utilize the watermarking techniques to make the process easier for embedding the data using key sessions with protection of user data.

The paper has structure as follows, in section 2 the related study and research will be discussed and section 3 is focused on the proposed model and its application process. Section 4 discussed about the evaluation of security schemes and concept of the two factor authentication system and concluded with section 5 with merit and demerits of schema through the direction of future enhancement.

## 2. PROBLEM STATEMENT

The problem statement for two factor authentication process proposed in the communication

system would have a weak security which leads to the data access with single authentication factor. The sensitive data about user will be leaked to breaches due to attacks like phishing, theft of passwords, etc., therefore proposed model with highly preserved two factor authentication system is necessary for enhancing data protection based on the parameters like knowledge and possession factors for accessing the user's sensitive data.

## 3. RELATED WORKS

In this section, two way factor of authentication is discussed with various researchers proposed with different models for enhancing the security to communicate in the open environment. In the digital era, user has to handle two different factors for data communication were the factors are biometric and authentications which is effective and transparent to the users.

In [1] author proposed applied combined facial recognition with RFID techniques for increasing the security accuracy of smart home application service to the user. The system authentication performance has the higher accuracy and the time taken to process smart things with minimum access using RFID technology for smart door open by identifying the experiment involved. The convenience will be reduced and the safety evaluation of the model is not completed. The similar approach will be proposed using same technology by analyzing the security method through BAN logic to protect the attacks with additional user validation action.

Kumar, et.al., [2] proposed an authentication schema for remote access to smart home by using one way hash functions using XOR operations with symmetric and asymmetric methods. The ROR model for security verification is used by AVISPA tool for biometric access which is not transparent to the users for causing the problem. Sensor networks which will be served in the medical field will have a higher security with authentication mechanism based on shared key techniques because of requiring higher data protection.

In [3], author has proposed two factor authentication systems based on the secret and shared key techniques between the user gateway and sensor with resilient ECC based three factor authentication protocols for better key establishment. By increasing the key length or implementing the public key techniques the processing and protecting time will be reduced and communication will be done in a rapid way.

Kamalraj, et.al., [4], implemented the security techniques during media transmission and storage of data which can be manipulated for illegal access by the third party user. Therefore, watermarking is a concept which protects the vulnerable data in the digital field against data tamper and the proposed methods are considered it holds the enhanced security. By proposing the watermarking algorithm based on lossy compression method to ensure the authentication of forgery detection [5]. The cryptography based technology helps to protect the data like bit pair match watermarking model using spatial domain techniques and the symmetric key cryptography is used to encrypt the data for protecting from the illegal access on communication channel. Watermarking techniques will helps to improve the security level by reducing the raise of security attacks in the network and it will also leads to avoid the exposing process of embedding the bits about image from the attackers or illegal access [6]. And the block based image watermarking system is proposed with algorithm generated the two

different keys using diffie hellman key exchange for identifying the location of the cover image to embed the watermark data with the applicability of watermarking techniques with user data transmission will leads to reduce the data quantity is transferred. Based on the discussed related works, two factor authentication schemes will supports the user convenience and lightweight protocol with enhanced security levels are completely known. Watermarking technique is described and the embedding process using random key generation is discussed with user image. It did not encrypt the user sent messages and will not perform any test assessments. For improving the security and privacy of the data, users have to validate the both user device and gateways of through were the data is communicated.

## 4. COMPARATIVE STUDY ABOUT 2FA (TWO FACTOR AUTHENTICATION)

Table 1: Merits and Demerits of existing research on two factor authentication system

| Author | Method proposed | Merits | Demerits |
|---|---|---|---|
| Ogi, Dono, et.al., [2020] | RFID +LBP algorithm | Higher security | User perception |
| Chisthi, et.al., [2022] | MFA | Low risk | Dependence of second factor |
| Ozkan, et.al., [2020] | RSA model | Highly flexible | Change of resistance |
| Gordin, et.al., [2019] | TOTP + QR based model | Compliant | Integration complex |
| Reimair, et.al., [2023] | CrySIL features proposed | Minimal process | Data processing time is larger |
| Joshi, et.al., [2021] | 3D Virtual ATM scheme | Certificate validation will be done | Time taken is larger |
| Gorman, et.al., [2023] | User ID collection for protection | Biometric enhanced for verification | Low authenticity level |
| Mariano, et.al., [2024] | TLS/SSL scheme | Strong key generation | Time taken for verification |
| Patrick, et.al., [2022] | SMS based scheme | OTP verification | Phishing attack possibility |
| Micheal, et.al., [2023] | Google verification process | Email validation | Tough to access validation process every time |
| Subhashini, et.al., [2021] | Multimodal mobile authentication | Static passwords | Weak links |
| Nancy, et.al., | HMAC based key | OTP verification | Low in accuracy |

| | | | |
|---|---|---|---|
| [2022] | generation | | |
| Moona, et.al., [2021] | Security model on ATM | Flexible and highly secured | Cost effective |
| Mohammed, et.al., [2020] | Multilayer factor authentication | 5 levels of authentication | Need improvement in layering |

## 5. PROPOSED MODEL

In this section, the techniques about the two factor authentication and security gateways are discussed in detailed with algorithms and its notation process. In the above figure 1, the proposed two factor authentication system model gateway is illustrated and the system is deployed with the security scheme which composes user data recognition with hardware identification model. Facial recognition authentication will ensure the validity of user to access the system when it will find the access is legal from the database located in the gateway. It will allow the user to access the system easier but the illegal accesses may be lead to lower security layers and privacy violations. To overcome the listed risks, the session of connection with internet will be used to protect the user data which is transmitted in between the users and security gateway. An encrypted user and their authentication data are embedded in a single encrypted message which will be exchanged using watermarking techniques with n number of authentication procedures based on the packet size of data will be reduced significantly with lightweight authentication protocol.

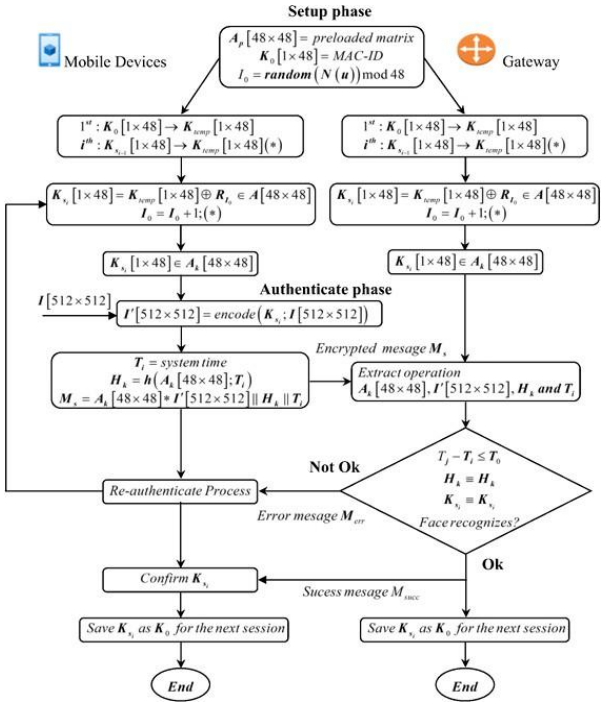


Figure 2: Two Factor authentication setup process

From the above figure 2, the process of setup phase is discussed with gateway collected the MAC address of user smart device and user data as image and store it to the databases such as image and key dataset. The MAC address which is collected in the earlier stage will be the 48 bit length data stored on user smart device and gateway to use the setup initialization process with key denoted as K0 which will be denoted as K0 [1 x 48]. The gateway and user phase will mutually record the data in the following manners,

1. Initialize key k0 [1 x 48]
2. Network size are indicated in random number with maximum number of devices, N(u)
3. Pre-loaded binary matrix is used as Ap [48 x 48]
4. In user and gateway process left bit shift algorithm is processed.

The data in the form of image stored at gateway will be considered for the matching of data by following the parameters and the proposed study will use the standard support vector machine algorithm for data recognition process. Also, the registration phase has three major steps and the cloud user can register themselves to cloud server as follows,

1. User can register with individual ID's and server will validation process will be started to verify all the provided information is valid or not.

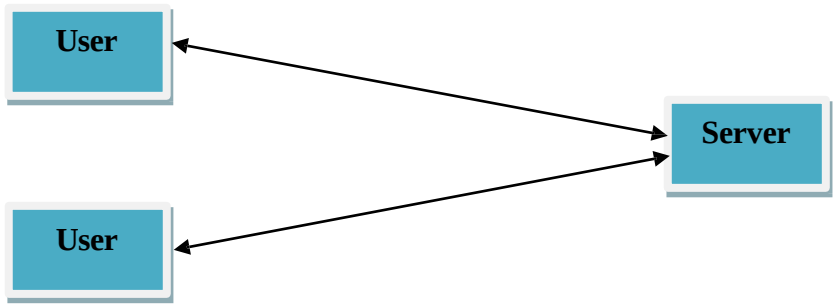


Figure 3: User registration process with server

2. The user will re-enter the valid data received from server for authentication process and keys are generated for establishing the communication securely to the server.

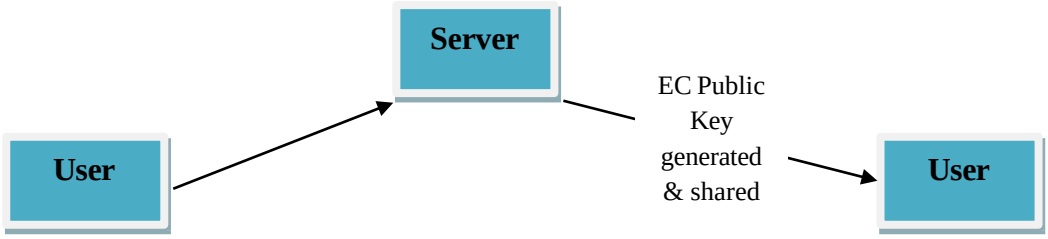


Figure 4: Key generation after registration and validation

3. The client generated password and requested service type is analyzed and duration is calculated and forward an entire data to the server with shared server based key in a highly secured manner.

Enccs_pk {H(user ID) || H(secured password) || nonceX}

After a successful registration of user record and password generation process the server will receive the security password and further details like service type, duration taken, etc., for processing the tasks. All the user credentials are recorded in server database with high security and certificate of cloud will be generated which consists of user details and lifetime of process, all those entire recorded information will send back to the user in an encrypted format. The certificate generation will be performed based on the private key and the data is again encrypted in double on receiver side, where the user will decrypt it using the server public key.

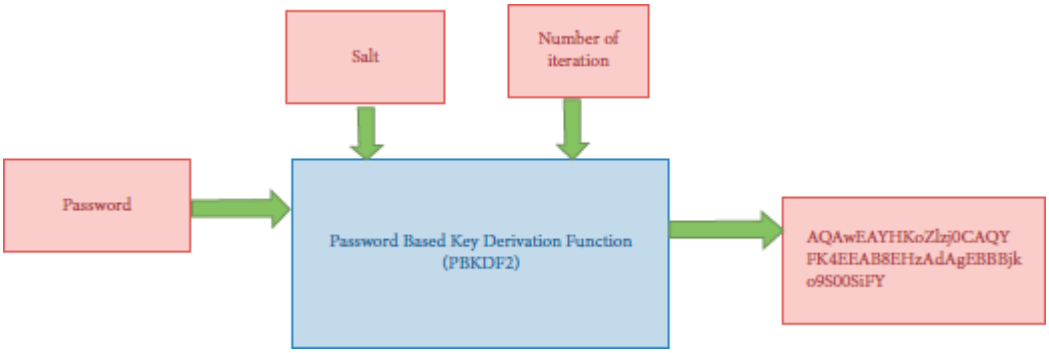


Figure 5. Security based two factor cloud scheme

The first factor of cloud authentication during the user request will be processed with cloud platform and it will be consist of database server and a web. All the server based data will be authenticated by database in the server against registered records upon the authentication confirmation which is sent back to cloud server for better communication to the user.

Encrypted message = Encrypted cloud server_public key{H(user ID || H(password)}

Cloud receive encrypted message and decrypt the data for verification of digital signature and after the successful verification the cloud server will initiated to send the verification data to registered used with enrolled data and waits for a allot time slot for the user to approve the authenticity of the signal received from the server.

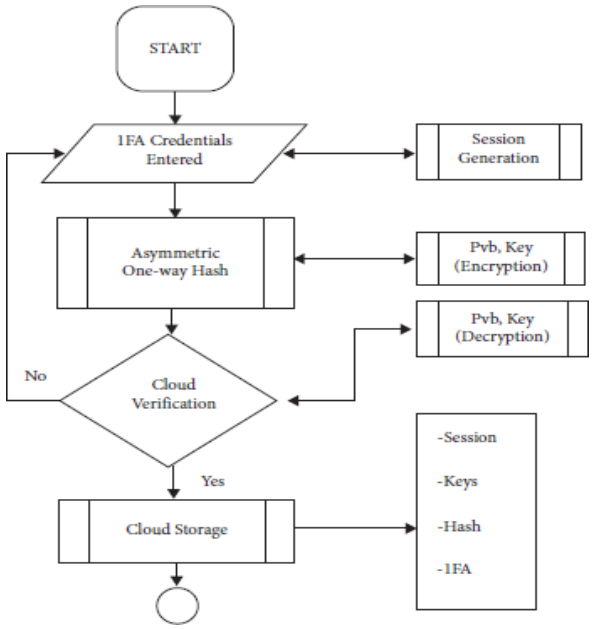


Figure 6: One factor authentication

After the one factor authentication, an user will be requested to verify the two factor authentication through application and the cloud database will reverify both the factors and send the confirmation of verification rejection of request back to the user for re-verification.

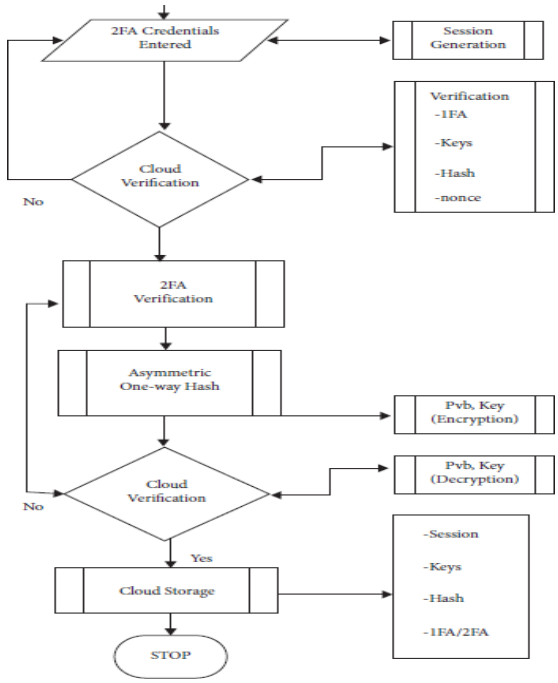


Figure 7: Two factor authentication process

One factor authentication process got verified and the user is prompted to verify for two factor authentication through an application and the cloud server will re-verify the both factors for confirmation and cloud will give grants to access the cloud.

Encrypted message = Encrypted cloud server_public key {H(cloud certificate) || H (data 1) || H (data2) || nonceY}

Table 2: Authentication approach with security level.

| S.No | Approach/ Scheme | Efficiency | Security level |
|---|---|---|---|
| 1. | Password based approach | High (<100ms) | Low security (guess attack- offline) |
| 2. | ECC based approach | Moderate (100- 500ms) | Medium security (impersonation attack) |
| 3. | Attribute based approach | Low (>500ms) | Strong security (privacy property) |
| 4. | PACE based approach | Low (>500ms) | Strong security (key generate) |
| 5. | Identity based approach | Low (pairing verify on user side) | Strong security |
| 6. | Zero knowledge based approach | Moderate (100- 500ms) | Strong security |

Behavior techniques for enhanced security prediction:

The behavior techniques are measured for some human behavior traits as signature, keystroke, and accuracy.Signature used in a bank industry in the past will be used for verification of the identity of the user for validation. Keystroke technique is a measure of person related to the work with keyboard operation which will be used to monitor the style of accessing the keyboard with few parameters such as keystroke between each time, number and frequency of errors and the pressure made on keys, etc., will be considered as the method of identify the user validation. Accuracy rate is predicted in the biometric models with two different parameters as follows,

False rejection rate = false rejection/ total rejection False acceptance rate = false acceptance/ total attempts

The proposed authentication scheme will perform some algorithm techniques as authentication phase like,

Step 1: User create the session key and insists to send the message which is encrypted Ms to the gateway.

Step 2: Gateway will generate the session key along with embedded key matrix process.

Step 3: It will verify the authentication parameters for validation.

Step 4: Every process will be notified to the user through message from the gateway server.

| |
|---|
| Algorithm: User generate session key and encrypted message ($M_S$) to the gateway |
| Input: Key $K_0$, matrix $A_p$, random number $i_0$, user face image I[512 x 512] ==user data == preloaded random matrix. |
| Session 1: $k_0$ [1 x 48] == MAC ID;$i_0$ == random (N(u)) mod 48; $i_0$ == ($i_0$ + 1) mod 48 |
| Output: encrypted message $M_S$ = $A_k$ [48 x 48] * I' [512 x512] ‖$H_k$‖$T_i$ |
| Start |
| Left shifting $i_0$ bits to create a key |

Session key $K_S$ from $K_{temp}$ and matrix $A_P$:$K_S$[1x48]-$K_{temp}$[1x48]+$RI_0$[1x48]$\in A_P$[48x48] created Create embedded key matric $A_k$: $A_k$[48x48] - $K_S$[1x48] + $A_P$[48x48]

Use $K_S$ for encoding the matrix I[48x48] to matrix I'[48x48]: I'[512 x512]-encode($K_S$:I[512x512])

Time stamp created $T_i$ - $T_i$= current time of the system to calculate the transmitted packet time. Create hash key to embedded key matrix $A_k$ for the enhanced security with integrity of key matrix $A_k$ and session key $K_S$: $H_k$-h($A_k$[48x48], $T_i$)

Encrypted message $M_S$ along with $A_k$ and $H_k$: $M_S$-$A_k$[48x48] || * I' [512 x512]||$H_k$||$T_i$ Transmission of data to the gateway and wait for $T_{timeout}$ for acknowledgement generation: $T_t$- $T_{timeout}$; $T_j$-$T_i$-$T_t$

If acknowledge = $M_{err}$ then Return to step 3

Else {acknowledge- $M_{success}$}

Next step End if

Store $K_S$ for the next step of authentication session

End

Algorithm: user process for response message from gateway

Input: received message ($M_{err}$, $M_{success}$)

Output: authentication for confirmation

Start

Receive acknowledgement message If acknowledgement = $M_{err}$ then,

Verification process repeated for re-verification Else [$M_{succ}$ = decode($K_S$, $M_{success}$(s))

End if

Confirm $K_S$ is safe to access end

For the analysis of security, user has to evaluate the strength of the security using authentication scheme proposed with security protection against security attacks, evaluation of security using BAN logic model, and using of simulation models like AVISPA for enhanced protection of data.

Existing session generation key process:

In the multi session security process two different users will execute the session key generation protocol at the same time and met with different users to run the n number of times. It will enhance the protocol layer to be secured with single process between two different parties which will leads to enhanced security level.

Proposed session keys required to meet some parameters like confidentiality, integrity, authentication, efficiency, dynamic security, scalability with restricted lifetime. It also some process to generate session key based on the key exchange protocol whereas two different users should accept the exchange key securely with random number generation to create a unique key for the session. Keys are combined and it will be derived from master key using encryption algorithms with strong encryption process to ensure the security level of the data. The validation process will start accessing the data and session will initiated for allotted time period only.

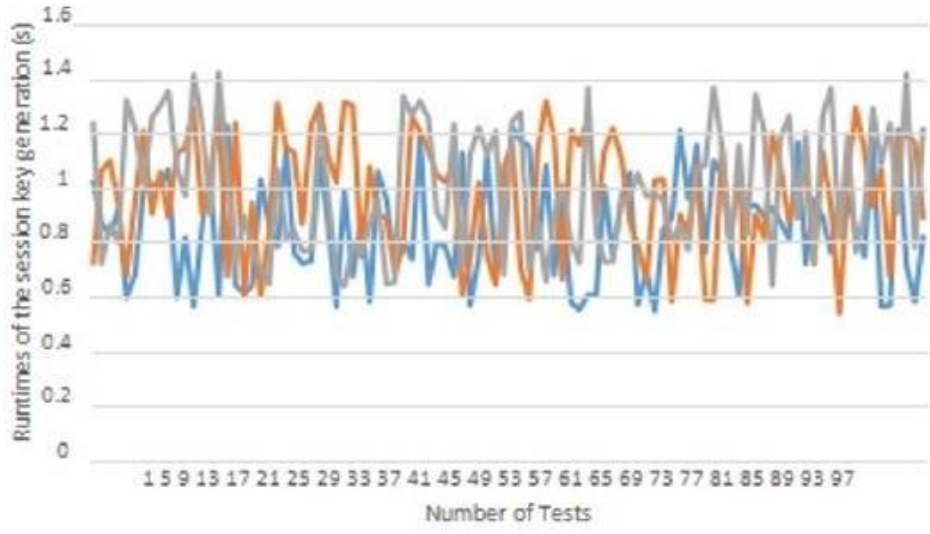


Figure 8: Session key generation process

For the better authentication process, the session key generation on user device is tested by capturing the data using camera, the image is encrypted and send the authenticated message (Ms) to the gateway. From the gateway it helps to recognize the user data by applying the SVM algorithm on image database collected and stored as input data which will be used to access the session key. Finally, time taken to encrypt the data and session key generation will be calculated using different techniques and processes of algorithms.

## 6. CONCLUSION

In the two factor authentication system, the level security is increased and it will be considered as the future security measure which will be considered as best authentication methods for most valuable online communication techniques such as banking transaction and any other institution transaction process will be considered as most secured and required security process. In the past digital banking process, all the online transaction will be done through with security password, later it will be enhanced with one time password system for improved security level. Moreover, this two factor authentication system will be considered as user friendly process and it should be known to all the users with little knowledge for protecting their data which is easy to access and highly flexible to communicate with database which is unbreakable. In this study work, we revealed that users can found two factor authentication enabled web applications are available for usage with several flaws, similarly the token process of this authentication methods are tough to access and read which is stressful to the humans. The automatic authentication process using wearables will helps to remove the need of users to convey the data for validating it, such smart devices will reduce the user interaction to perform the two factor authentication process easier.

## References


1. Ogi, Dono, et.al., “Two factor authentication based RFID technology for face recognition system using LBP algorithm”, International conference on ICT for smart society (ICISS), IEEE, 2020.
2. Das, Kumar, et.al., “Secured remote authentication for smart home access with key model”, IEEE Transaction on secure computing, pp. 391-406, Volume 2, Issue 17, 2017.
3. Kumari, et.al., “Enhanced two factor authentication protocol methods to health care applications using wireless medical sensor networks”, Multimedia systems, volume 23, issue 2, pp. 195-205, 2019.
4. Kabir, et.al., “Enhanced low bit rate image watermarking system with tamper detection model”, SN applied science, Volume 3, issue 4, pp. 1-17, 2021.
5. Nayak, et.al., “Secured watermarking system using cryptography and bit pair matching”, Journal of king Saud university- computer and information sciences, volume 33, issue 5, pp. 552-561, 2021.
6. Aparna, et.al., “Image watermarking system with hellman key exchange algorithm”, procedia computer science, volume 6, 2022.
7. S. Prabhakar, et.al., “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy Mag., volume 1, issue 2, pp. 33–42, 2023
8. S. Wiedenbeck, et.al., “Design and longitudinal evaluation of a graphical password system”. International journal of Human-Computer Studies, volume 63, pp.102-127, 2024.
9. Swathi, Jagannatha Reddy, “Authentication Using Persuasive Cued Click Points”, International Journal of Engineering Research & Technology (IJERT), Volume 2, Issue 7, 2023.
10. Sonia Chiasson, “Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points”, IEEE Transactions on Dependable and Secure Computing, volume 03, issue 3, 2022.
11. L. Jones, et.al., “Towards Understanding User Perceptions of Authentication Technologies,” Proceeding of ACM Workshop Privacy in Electronic Society, 2023.
12. Fatehah M.D, et.al., “Educating Users to Generate Secure Graphical Password Secrets: An Initial Study”, IEEE society, 2023.
13. Abdul Hanan Abdullah, et.al., “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”, IEEE, 2019.
14. Rekha Sharma, “Securing text & image password using the combinations of Persuasive Cued Click Points with the help of Improved Advanced Encryption Standard”, International Conference on Advanced Computing Technologies and Applications, 2022.
15. Madhuri Achmani, et.al., “Two Level Authentication System Based on Pair Based Authentication and Image Selection”, IJRASET, Volume 4, Issue 4, 2022.
16. N. S. Joshi,"Session Passwords Using Grids and Colors for Web Applications and PDA", International Journal of Emerging Technology and Advanced Engineering, 2023.
17. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), volume 2, pp. 467-472, 2023.
18. Mohd. Et.al., "A Graphical Interface for User Authentication on Mobile Phones", The Fourth International Conference on Advances in Computer-Human Interactions, 2022.