Implementation of Novel One Time Password Authentication Algorithm to Provide Better Security and Easy Generation

[1]Dr. Prakash Kuppuswamy, [2]Dr. Rajan John , [3]Ahmed Ali Shaik Meeran , [4]Dr. Sayed QY Al Khalidi , [5]Vijaya Varshini

[1]Computer Science Engineering
SRM University, Delhi-NCR, Haryana, India.
[2]Department of Computer Science
Jazan University Jazan, KSA.
[3]Department of Information Technology
Jazan University, Jazan, KSA
[4]Department of Information Technology
King Khalid University, Abha, KSA
[5]Computer Science Deparment
Bharathiyar University, Coimbatore
Tamil Nadu, India.

Abstract

In today's digital age, ensuring secure access to systems and services is of paramount importance. One-time password (OTP) generation techniques have emerged as a powerful tool for enhancing security and mitigating the risks associated with traditional password-based authentication methods. A one-time password is a temporary code that is generated on-demand and only valid for a single authentication session. Unlike traditional passwords that remain the same over a prolonged period, OTPs provide an additional layer of security by introducing a time-based or algorithm-based factor into the authentication process. This paper provides a comprehensive overview of OTP generation techniques, their advantages, and their applications across various sectors. Additionally, we will explore the recent advancements in OTP generation techniques and their potential implications for the future of secure authentication. In today's digital world, the importance of secure authentication cannot be overstated. One-time password (OTP) technology has emerged as an effective way to enhance security by providing an additional layer of protection for access to systems and services. This article aims to explain how OTPs work, their underlying principles, and the benefits they offer in ensuring secure authentication.

Keywords: One Time Password, HOTP, TOTP, Authentication, Symmetric key algorithm etc.,

1. Introduction

In today's digital era, where personal data and online security are of paramount concern, the need for robust authentication methods has never been more vital. One such method that has gained popularity is the "One-Time Password" (OTP) [1-3]. An OTP is a unique temporary code sent to a user's device that helps verify their identity during online transactions or when accessing sensitive information [4,5]. In this introduction explores the concept of OTPs, their significance in enhancing security, and their usage in various industries.

A one-time password (OTP) is a single-use code generated for authentication purposes. It provides an extra layer of security by requiring users to enter a unique code alongside their regular login credentials [6,7]. OTPs are typically sent to the user via email, SMS, or through specialized mobile apps.OTP technology works on the idea that passwords can be easily stolen, guessed, or intercepted, exposing users to potential threats from hackers and cybercriminals [8-10]. By generating a temporary code that expires after a single use, OTPs mitigate the risk of unauthorized access even if a password is compromised. The

temporary nature of OTPs assures users that the code will not be reused and provides an additional layer of security [11,12].

Symmetric key algorithms play a vital role in ensuring secure and efficient communication in various information systems. These algorithms form the foundation of cryptography by utilizing a single shared secret key for both encryption and decryption [13,14]. This article aims to delve into symmetric key algorithms, exploring their working principles, strengths, weaknesses, and real-world applications.Symmetric key algorithms, also known as secret-key or private key algorithms, employ a shared secret key to encrypt and decrypt data. This key is known only to the entities involved in the communication process, ensuring confidentiality. The encryption process involves converting plaintext data into ciphertext, making it unreadable to unauthorized parties [15,16]. The decryption process, on the other hand, converts the ciphertext back into its original plaintext form.

The strength of symmetric key algorithms lies in their speed and efficiency. They are designed to handle large volumes of data quickly, making them ideal for real-time communication and high-performance applications. Some well-known symmetric key algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), and Rivest Cipher (RC4) [17-19].

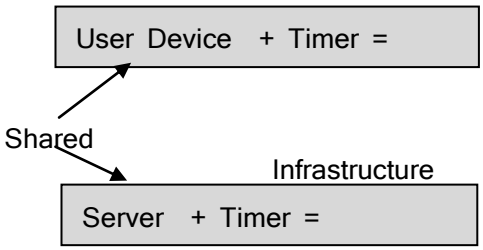

Figure1. General OTP structure

1.1. OTP

OTP, or one-time password, is a security measure used to validate a user's identity during authentication processes. As the name implies, an OTP becomes invalid once it has been used, making it a reliable method for preventing unauthorized access. OTPs are often used as a second factor in dual-factor authentication systems, alongside traditional password-based login mechanisms. An OTP is typically generated by an algorithm and sent to the user's registered device via SMS, email, or through authenticator mobile applications. It is a randomly generated numeric or alphanumeric code that expires after a short period of time or upon use. Upon receiving the OTP, the user must enter it into the designated authentication field to gain access to the desired application or system [20,21].

1.2. TotP

TOTP, or Time-based One-Time Password, is a variation of OTP that adds an additional layer of security by incorporating time synchronization. Unlike traditional OTPs that expire upon use, TOTPs have a predefined expiration timeframe, generally 30 seconds. This time synchronization aspect ensures that both the generating system and the verifying system have synchronized clocks, making the password valid only for a specific time frame. The TOTP algorithm combines the current timestamp and a shared secret key to generate a one-time password. This shared secret key is securely exchanged or preconfigured between the user's device (typically a mobile app) and the authentication server or service provider. By incorporating time synchronization, TOTPs provide an added layer of security against potential replay attacks or password interception attempts.

TOTPs are commonly used in conjunction with authenticator mobile applications, such as Google Authenticator or Authy. These apps generate TOTPs that constantly update based on the synchronized time and shared secret key. Users can simply open the app, view the current TOTP, and enter it when prompted during the authentication process [22, 23].

1.3. HOTP

HOTP, or HMAC-Based One-Time Password, is another variation of OTP that uses a Hash-based Message Authentication Code (HMAC) to generate

one-time passwords. Unlike TOTP, HOTP passwords are not time-dependent but are instead generated based on a counter value. This counter value increments with each successful password verification, ensuring that each password is used only once. HOTP algorithms use a shared secret key and a counter value as inputs to an HMAC function, resulting in a unique one-time password for every increment. The shared secret key is securely exchanged or preconfigured between the user's device and the authentication server. Each time the user needs to authenticate, the counter value is increased, and the corresponding HOTP is generated.

HOTP is commonly used in scenarios where time synchronization might not be feasible or desired, or in situations where password reuse needs to be prevented. This method is particularly useful when used with physical tokens such as key fobs, where a user simply presses a button to generate the next HOTP [24-27].

The paper aims to provide a comprehensive understanding of one-time password (OTP) generation techniques, their underlying principles, and their applications. It will discuss the advantages of OTPs over traditional password-based authentication methods, exploring the various OTP generation techniques such as TOTP, HOTP, challenge-response OTPs, and biometric-based OTPs. Security considerations, implementation challenges, and real-world case studies will also be covered. Furthermore, the paper will highlight recent advancements, potential future directions, and the challenges and limitations faced by OTP generation techniques. By the end, readers will have a deep understanding of OTPs and their role in enhancing security in the digital age.

2. Background Study

Gowda (2016) There are several cryptographic algorithms, but Caesar Cipher is the oldest. Despite the existence of much more secure algorithms, the Caesar cipher algorithm continues to be the fastest owing to its simplicity. This algorithm can, however, be cracked very easily. It does this by replacing every character of a message with the same predetermined fixed character. There are a few changes that can be made to the algorithm to enhance its security feature. Using the Diffie-Hellman key exchange scenario, this paper proposes an enhancement to the existing algorithm, which uses simple mathematics to ensure that data encryption is much more secure. Using the Diffie-Hellman method, a private shared key is obtained by moderating it with 26 to obtain a value less than or equal to 26, then the current character is taken, and the key value is added to the current character to obtain a new character [28].

Vikas Wasson, Bikrampal Kaur (2021) From the electronic democratic machine to online shopping, system frameworks are unavoidable in our general public. The purpose of data security is to ensure that information is classified, accessible, respectable, and secure whereby both the sender and recipient should ensure secure transmission of information between source and destination hubs using encryption and decoding methods. As part of the present paper, key appropriation RSA techniques are applied to the multi-throwing situation, while mobile specially appointed networks (MANETs) are remote correspondence networks that do not require any prior arrangement or cluster of administrations. Each key administration expert receives a new portion of the discharge key occasionally, dispersed throughout the system. Consequently, numerous efforts have been made to adapt key administration specialists' tasks to MANET's dynamic environments and to distribute the assignments among the hubs. It is more effective to use an unbalanced cryptosystem when the key usage process is based on a given assignment. For one-jump communication in versatile specially appointed systems, this paper proposes a new common confirmation and key administration convention [29].

Ariel Roy L. Reyes, Enrique D. FestijoRuji P. Medina (2018) This study introduces a novel modification of the Blowfish cryptographic algorithm, which takes advantage of its strengths but also supports 128-bit input blocks using dynamic selection encryption and reduces cipher function execution through randomly determined rounds. By adding an additional layer of security, the modification provides a more robust and resilient system against attacks by unauthorized

parties, making it desirable to use in applications with multiple users. As a result of the results and analysis conducted, it was apparent that dynamic selection encryption and dynamic rounds for cipher function execution introduced additional complexity and confusion to an adversary. It was also found that the proposed modifications had increased both the avalanche effect and integrity as well as reducing execution time without compromising the security features of the original Blowfish algorithm [30].

Khairul Muttaqin, JefrilRahmadoni (2020) The transmission and storage of data using electronic media requires a process that can ensure the integrity and security of the data with encoding. A data is encrypted when it is converted into a confidential format that cannot be read, and a data is decrypted when it is converted back to its original format. As the latest cryptographic algorithm standard, the Advanced Encryption Standard (AES) is used. Prior algorithms were not able to deal with the challenges of communications technology development very quickly. With a key length of 128 bits, AES encrypts and decrypts data blocks over 128 bits using the Rijndael algorithm. We used AES to encrypt and decrypt files in this study to demonstrate the effectiveness of this system [19].

K. Hazelwood (2018) The paper describes the hardware and software infrastructure that supports machine learning globally. There is a wide variety of models required in practice by Facebook's machine learning workloads. All layers of the system stack are affected by this diversity. Additionally, a large percentage of all Facebook data is processed through machine learning pipelines, creating significant challenges for distributing data to high-performance distributed training flows. For real-time inference, GPU and CPU platforms are also used, based on GPU and CPU platforms for training. Diverse efforts spanning machine learning algorithms, software development, and hardware design continue to be required to address these and other emerging challenges [31].

Prakash Kuppuswamy, Saeed Qasim Yahya Al Khalidi Al-Maliki, Rajan John, Mohammad Haseebuddin, Ahmed Ali Shaik Meeran(2023) In contrast to public and private key single encryption methods, hybrid encryption methods combine the encryption schemes of two symmetric keys or both symmetric and asymmetric methods. Many cryptographic algorithms are currently available on the market and claim to provide higher levels of data security. There are many hybrid algorithms that fail to provide customers with the level of security they expect and that are not capable of preventing every form of security threat. It is imperative in the digital age to develop novel and resilient security systems to protect digital data. An algorithm scheme that uses RSA and SSK is recommended. It combines the well-known Rivest Shamir Adleman (RSA) algorithm. In this study, a new symmetric SSK algorithm is proposed along with RSA to develop a better encryption method [32].

3. Problem Statement

While OTPs offer several benefits, it is important to address the challenges and potential vulnerabilities associated with their usage. Ensuring secure delivery of OTPs remains a significant challenge. SMS-based OTPs, for example, can be intercepted by attackers using techniques like SIM swapping or phishing. To overcome this, alternative communication channels such as email or specialized OTP apps are deployed.The rise of mobile usage has made mobile OTP applications a popular choice. However, the security of mobile devices is subject to vulnerabilities like malware and device theft. Encouraging users to secure their devices with strong passcodes, encryption, and regular security updates reduces the risk of compromise.

Human error poses a risk when entering OTPs. For example, users may accidentally input the wrong code, leading to errors in the authentication process. Displaying clear instructions and designing user-friendly interfaces can help minimize user error.Cybercriminals often attempt to deceive users into providing their OTPs through fraudulent emails, websites, or calls. Education and awareness campaigns are critical to help users identify phishing attempts and avoid disclosing their OTPs to unauthorized parties.To mitigate these challenges, organizations and service providers must implement stringent security

measures such as encryption, multi-channel delivery options, and behavioral analytics to detect anomalies and potential security breaches.

4. Proposed Method

Symmetric key algorithms support various encryption modes to handle different types of data and communication scenarios. The most widely used modes include Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), and Galois Counter Mode (GCM). ECB mode encrypts each block of plaintext individually, which can lead to security vulnerabilities due to identical plaintext blocks producing identical ciphertext blocks. CBC mode addresses this issue by XORing each plaintext block with the previous ciphertext block before encryption. CTR mode converts the secret key into a stream cipher, while GCM mode provides both confidentiality and integrity protection. The process of using OTPs for authentication typically involves the following steps:

4.1. OTP Generation

When the user attempts to access a system or service, they are prompted to enter an OTP. The OTP can be generated by an app installed on their device, received via SMS or email, or generated by a hardware token.

1) Choosing Random 4bit code
2) Multiply 4 bit integer number random selected natural number
3) Calculate with modulo 37
5) OTP =(4-bit integer * n)mod 37

4.2. Verification

The OTP entered by the user is sent to the server for verification. The server applies the same OTP generation algorithm using the shared secret key associated with the user's account. If the OTPs match, the user is granted access. Otherwise, the authentication attempt is denied.

1) Multiply received text with inverse key
2) Calculate with modulo 37
3) Remainder is Revealed Text or Plain Text PT = $(CT*n^{-1})$mod 37

4.3. Access verification method

1) Verification stored message calculate with 'k'
2) Calculate with modulo 37
3) Now user authentication variable and accessing variable same then access granted

5. Designing Architecture

Symmetric key algorithms employ various working principles and encryption modes to ensure data security. The most common working principles include substitution, permutation, and combination techniques. Substitution involves replacing characters or bits with different ones, while permutation involves rearranging the order of characters or bits. Combination techniques combine substitution and permutation to enhance the level of security.

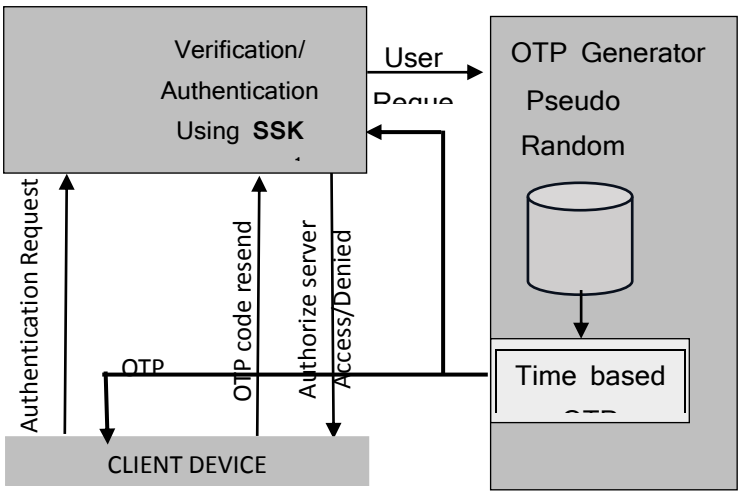

Figure 2. SSK OTP Architecture

The purpose of password security is to identify network security threats, coordinate threat response, and secure payment transactions. Through external networks, it will facilitate commercial transactions between customers and service providers. Fig. 2 illustrates the main architecture components that are connected to the server authentication, the OTP generator, and the client devices. After the client connects to the server, it sends a request to the server, which redirects to the pseudo random number generator. The pseudo random generator generates the number and sends it to the client's registered device at the same time that the SSK algorithm generates the random number to send to the authentication verifier of the client's OTP. A cross-verification of the OTP number is performed by sending the inverse of the random number to the server side. A server will allow authenticated devices to access if the OTP and SSK random numbers on the client side are equal, and if the inverse random numbers on the authentication server are equal, then the client will not be able to access.

6. Implementation

Symmetric key algorithms find applications in various domains, securing communications at different levels. They are extensively used in secure messaging applications, virtual private networks (VPNs), and secure email systems. Symmetric key algorithms also play a role in securing data at rest, such as encrypting data stored on portable drives or cloud storage.Moreover, symmetric key algorithms are employed in securing wireless communication protocols, securing data transmitted over computer networks, and protecting sensitive information in databases. Their speed and efficiency make them suitable for securing large-scale systems and reducing computational overhead.The system is core i8 intel 128 bit Windows 10, 16 GB RAM used.

Table 1. 4-Digit OTP process using SSK

4 Digit OTP	Mod37= PT	CT=(PT*n) mod37	PT=(CT*n^{-1}) mod37
1234	13	2	13
4321	29	13	29
3214	32	22	32
1243	22	29	22
2343	12	36	12
6671	11	33	11
3422	18	17	18
6688	28	10	28
4312	20	23	20

We have chosen 4 digit OTP and 6 digit OTP sample numbers for implementation of OTP generation, as shown in table 1 and 2. In the previous section, we discussed that when a client initiates a request, the server redirects it to the OTP generator. During OTP generation, the generator sends 4 digits or 6 digits to the client, which is then submitted to the server. The authentication verifier checks the sender OTP and pseudo random OTP using the random number that has been mentioned on the above table as part of our verification process.

Table 3. 6-Digit OTP process using SSK

6 Digit OTP	Mod37= PT	CT=(PT*n) mod37	PT=(CT*n^{-1}) mod37
666343	10	30	10
345634	17	14	17

123456	24	35	24
654321	13	2	13
845632	34	28	34
678799	34	28	34
777231	9	27	9
869923	16	11	16

7. Discussion

Symmetric key algorithms play a fundamental role in ensuring secure and efficient communication by employing a shared secret key for encryption and decryption. Their speed and efficiency make them ideal for real-time communication, high-performance applications, and resource-constrained environments. While they offer simplicity and speed, key management and secure key distribution remain a challenge. Nevertheless, symmetric key algorithms continue to be a cornerstone of modern cryptography, protecting sensitive information across various domains.

The main strengths of symmetric key algorithms include speed, efficiency, and simplicity. They can encrypt and decrypt data quickly, making them suitable for real-time communication and resource-constrained environments. Additionally, symmetric key algorithms are straightforward to implement and require less computational overhead compared to their asymmetric key counterparts.

Table 4. OTP Algorithm comparison

ALGORITHM	KEY SIZE	ITERATIONS	PROCESSING SPEED in(ms) 16 BIT LENGTH
MD5	128	4	22
SHA-0	160	80	20
SHA-1	160	80	24
SHA-2	256	80	28
SHA-3	512	24	32
SSK	16	1	8

As shown in Table 4, we compare the proposed new SSK algorithm with existing algorithms such as Message Digest 5 and Secure Hash algorithms of different versions. The above table of comparison states that key size and number of iterations are better than other algorithms that have been implemented in 16-bit messages or OTP numbers.

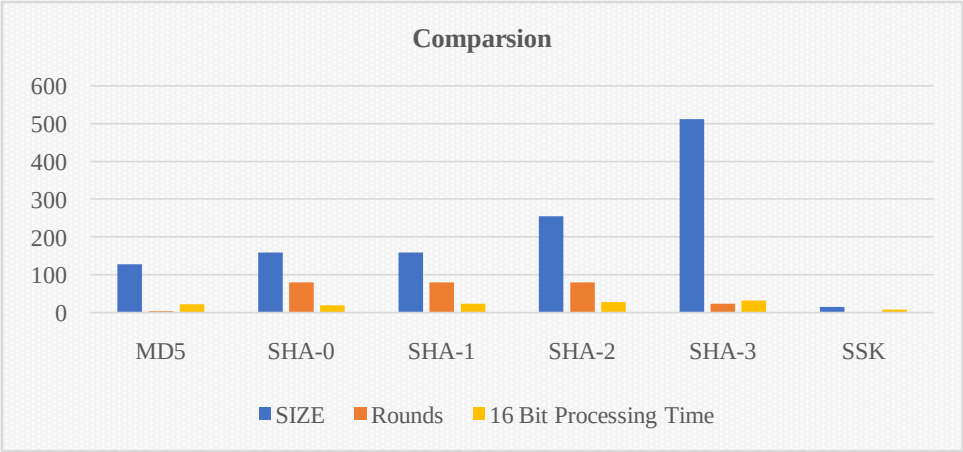

Figure3. Performance analysis chart

As shown in Figure 3, there is a performance analysis of various OTP algorithms with different metrics, including the key size, the number of processing rounds, and the length of the OTP.

8. BENEFITS OF THE SSK BASED OTP

Proposed Simple symmetric key (SSK) OTP algorithm offers several advantages over traditional password-based authentication methods:

8.1. Enhanced Security

The temporary nature of OTPs minimizes the risk of password theft or reuse. Even if an OTP is intercepted or compromised, it will be useless for subsequent authentication attempts.

8.2. Protection Against Phishing

OTP technology can mitigate the risk of falling victim to phishing attacks. Since OTPs are generated based on specific challenges or time intervals, they cannot be easily replicated by attackers attempting to deceive users into providing their credentials.

8.3. Compliance with Regulatory Standards

OTP technology helps organizations meet regulatory requirements for strong authentication, particularly in industries such as finance, healthcare, and government.

8.4. User Convenience

OTP technology offers a balance between security and usability. It provides an extra layer of protection without requiring users to remember complex passwords or follow frequent password update policies.

9. Conclusion

One-time passwords are an integral part of secure authentication in the digital age. By leveraging randomness, unpredictability, and time or challenge-based factors, OTPs enhance security and protect against various cyber threats. Understanding how OTPs work and their benefits is crucial for organizations and individuals seeking to ensure secure access to their systems and services.As cyber threats continue to evolve, the importance of robust security measures becomes increasingly evident. One-Time Passwords (OTPs) provide a valuable layer of protection against unauthorized access and identity theft, offering secure authentication for online transactions and sensitive data access. OTPs are being widely adopted across various industries, including finance, e-commerce, healthcare, and government services, to enhance security measures. While the adoption of OTPs brings several benefits, it is crucial to address the challenges associated with their usage. By implementing secure delivery channels, educating users about potential vulnerabilities, and continuously improving security measures, organizations can ensure the effective and safe deployment of OTPs.As the digital landscape continues to evolve, it is imperative for individuals, service providers, and regulatory bodies to embrace innovative security solutions like OTPs to safeguard personal information and build a safer online environment for all.

REFERENCES

[1] MohammadOnais Ahmad, Gautami Tripathi, Farheen Siddiqui, Mohammad Afshar Alam, Mohd Abdul Ahad, Mohd Majid Akhtar, Gabriella Casalino, “A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities”, MDPI, Journals Sensors, Volume 23, Issue 5, 10.3390/s23052757

[2] Sajaad Ahmed Lone, A. H. Mir, “A Stable and Secure One-Time-Password Generation Mechanism Using Fingerprint Features International Journal of Innovative Technology and Exploring Engineering (IJITEE)” ISSN: 2278-3075, Volume-8 Issue-9, July 2019

[3] Sarveshwaran, V., Chen, J.IZ., Pelusi, D.,“Artificial Intelligence and Cyber Security in Industry 4.0. Advanced Technologies and Societal Change”, Springer, Singapore, 2023. https://doi.org/10.1007/978-981-99-2115-7_3.

[4] Shanmugapriyan, Parthasarathy, Sathish, Prasanth, "Secure Electronic Transaction Using AADHAAR Based QR Code and Biometric Authentication," 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2022, pp. 1-4, doi: 10.1109/IC3IOT53935.2022.9767978.

[5] Ajish, S., Anil Kumar, K.S.,“Secure Mobile Internet Banking System Using QR Code

and Biometric Authentication, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies", vol 117. Springer, Singapore. 2022https://doi.org/10.1007/978-981-19-0898-9_60

[6] Papaspirou,Maglaras, Ferrag, Kantzavelou, Janicke, Douligeris, "A novel Two-Factor HoneyToken Authentication Mechanism," 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 2021, pp. 1-7, doi: 10.1109/ICCCN52240.2021.9522319.

[7] Theagarajan, Srinivansan, Alagesan, Kasinathan,Venkatesh, "IoT-Based Passenger Authentication System For Transportation Services," 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vellore, India, 2023, pp. 1-5, doi: 10.1109/ViTECoN58111.2023.10157579.

[8] Muhammad Shafiq, Zhaoquan Gu, Omar Cheikhrouhou, Wajdi Alhakami, Habib Hamam, "The Rise of Internet of Things: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8669348, 12 pages, 2022. https://doi.org/10.1155/2022/8669348

[9] Fang, Quintos,"Security Measures Applied on Digital Banking Towards Service Improvement Proposal", Journal of Business and Management Studies, 5(5), 47–77, 2023. https://doi.org/10.32996/jbms.2023.5.5.5

[10] Shreyansh Sharma, Anil Saini, Santanu Chaud hury, "A survey on biometric cryptosystems and their applications Computers & Security", Elseveir publication,Volume 134, November 2023, 103458

[11] Hussain, Muhammad Iftikhar, Jingsha He, Nafei Zhu, Fahad Sabah, Zulfiqar Ali Zardari, Saqib Hussain, and Fahad Razque. "AAAA: SSO and MFA Implementation in Multi-Cloud to Mitigate Rising Threats and Concerns Related to User Metadata" Applied Sciences 11, no. 7: 3012, 2021,https://doi.org/10.3390/app11073012

[12] Paul, Haldar,"UI Component and Authentication. In: Serverless Web Applications with AWS Amplify", Apress, Berkeley, 2023. CA. https://doi.org/10.1007/978-1-4842-8707-1_2

[13] S. N. Gowda, "Innovative enhancement of the Caesar cipher algorithm for cryptography", 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA), Bareilly, India, 2016, pp. 1-4, doi: 10.1109/ICACCAF.2016.7749010.

[14] Ako Muhammad Abdullah, Roza Hikmat Hama Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm",International Journal of Computer Applications, Volume 143 – No.4, June 2016.

[15] Chandel, Aggarwal,Mittal, Choudhury, "Comparative Analysis of AES & RSA Cryptographic Techniques", International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 410-414, doi: 10.1109/ICCIKE47802.2019.9004338.

[16] Ariel Roy, Reyes, Enrique,Festijo, Ruji, Medina, "Securing One Time Password (OTP) for MultiFactor Out-of-Band Authentication through a 128- bit Blowfish Algorithm", 10, No. 1, April 2018.

[17] B. Jan, H. Farman, M. Khan, M. Talha and I. U. Din, "Designing a Smart Transportation System: An Internet of Things and Big Data Approach," in IEEE Wireless Communications, vol. 26, no. 4, pp. 73-79, August 2019, doi: 10.1109/MWC.2019.1800512.

[18] Nikouei, Y. Chen, S. Song, R. Xu, B. -Y. Choi and T. R. Faughnan, "Real-Time Human Detection as an Edge Service Enabled by a Lightweight CNN," 2018 IEEE International Conference on Edge Computing (EDGE), San Francisco, CA, USA, 2018, pp. 125-129, doi: 10.1109/EDGE.2018.00025.

[19] Khairul Muttaqin, JefrilRahmadoni,"Analysis and Design of File Security System Advanced Encryption Standard Cryptography based", Journal of Applied Engineering and Technological ScienceVol 1(2) 2020: 113-123114

[20] Hanan Fahm, Noha Elkhateeb, “Proposed Model for Generation of One Time Password”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 11, November 2018.

[21] Kaustubh Chude, Aditi Karwa, Megha Sah,Tanmay Bhavsar, “Multi-factor Authentication for Physical Access”, International Journal of Scientific Research in Engineering and Management (IJSREM) Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930.

[22] Jackulin Sam JIni, K.Priyanka, J.Sathya, P.Sharmila, “Tenable Online Issue of Birth Certificate for Regime Conglomerate”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072, 2018.

A. Catalfamo, A. Ruggeri, A. Celesti, M. Fazio, M. Villari, "A Microservices and Blockchain Based One Time Password (MBB-OTP) Protocol for Security-Enhanced Authentication", IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 2021, pp. 1-6, doi: 10.1109/ISCC53001.2021.9631479.

[23] V. Parmar, H. A. Sanghvi, R. H. Patel and A. S. Pandya, "A Comprehensive Study on Passwordless Authentication”, International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1266-1275, doi: 10.1109/ICSCDS53736.2022.9760934.

[24] J. Dutson, D. Allen, D. Eggett and K. Seamons, "Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication”, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 2019, pp. 119-128, doi: 10.1109/EuroSPW.2019.00020.

[25] Das, S., Dingman, A., Camp, L.J.,“Two Factor A Two-Phase Usability Study of the FIDO U2F Security KeyFinancial Cryptography and Data Security”, FC 2018. Lecture Notes in Computer Science, vol 10957. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-58387-6_9

[26] Amritraj Singh, Kelly Click, Reza M. Parizi, Qi Zhang, Ali Dehghantanha, Kim-Kwang Raymond Choo, “Sidechain technologies in blockchain networks: An examination and state-of-the-art review”, Journal of Network and Computer Applications, Volume 149,2020, 102471, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2019.102471.

[27] S. N. Gowda, "Innovative enhancement of the Caesar cipher algorithm for cryptography”, 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, India, 2016, pp. 1-4, doi: 10.1109/ICACCAF.2016.7749010

[28] Vikas Wasson,Bikrampal Kaur, “Meta-analysis of distortions effects on quality of digital images using standard IQA datasets”, Journal of Discrete Mathematical Sciences and Cryptography 24:5, pages 1545-1558.

[29] Ariel Roy L. Reyes, Enrique D. Festijo, Ruji P. Medina,“Securing One Time Password (OTP) for MultiFactor Out-of-Band Authentication through a 128- bit Blowfish Algorithm”, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 10, No. 1, April 2018.

[30] K. Hazelwood, "Applied Machine Learning at Facebook: A Datacenter Infrastructure Perspective”, IEEE International Symposium on High Performance Computer Architecture (HPCA), Vienna, Austria, 2018, pp. 620-629, doi: 10.1109/HPCA.2018.00059.

[31] Prakash Kuppuswamy, Saeed Qasim Yahya Al Khalidi Al-Maliki, Rajan John, Mohammad Haseebuddin, Ahmed Ali Shaik Meeran, “A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm”, Bulletin of Electrical Engineering and Informatics, Vol.12, No.2, April 2023.

AUTHORS BIOGRAPHY

Dr Prakash Kuppuswamy, Associate Professor, Computer Science Engineering Department, SRM University, Sonepat, Haryana. Doctorate from Dravidian University. He has published 40 International Research journals/Technical papers and Participated in many international Conferences in Maldives, Libya and Ethiopia and Saudi Arabia. His research area includes Cryptography, Bio-informatics and E-commerce security, Cloud Security etc

Dr. Saeed Q. Al-Khalidi Al-Maliki, is a faculty member in the Department of Management Information Systems (MIS), College of Business, King Khalid University (KKU), Saudi Arabia. He was a Member of the Consultative Council (Shura Council) of the Kingdom of Saudi Arabia for four years between 2016 - 2020. He has worked as a vice-dean and then as a Dean of Library Affairs at KKU. Currently, he works as a vice-dean for the Research and higher Studies, College of Business, KKU. Dr. Al-Maliki's research interests include IS development, approaches to systems analysis, and the early stages of the system development process, IT/IS evaluation practices, e-readiness assessments, GIS issues, ICT, and e-government issues.

Dr John Rajan is Assistant Professor, Department of Computer Science, College of Computer Science & Information Technology, Jazan University, KSA. Ph. D awarded by Karunya University. He has published 20 International Research journals/Technical papers and participated in many international Conferences

Ahamed Ali Shaik Meeran, Department of Information Technology, College of Computer Science & Information Technology, Jazan University, KSA. Master Degree obtained from Andhra University, Visakhapatnam, A.P, India. Specialized in networks and Server Administration.

K.P. Vijaya Varshini, Post Graduation Students of Bharathiyar University, Research Interest in Data Science, Image Processing, Machine Learning Operation Research etc.,