DOI: https://doi.org/10.67897/njma.2025.ouxb5w0m



Nigerian Journal of Mathematics and Applications
Volume **35**, (2025), 01 – 15. *Printed by Unilorin press*
©*Nig. J. Math. Appl.* *http : //www.njmaman.com*

Double-Blinded One-Time-Password Key Generation for Authentication in Internet of Things (IoT)

Adisa Jamiu Saka[1], Segun Aina[2], Omolara Aminat Ogungbe[3], Kehinde Adam Olurode[4], Ishaya Peni Gambo[5], Oluwafemi Joshua David[6] and Kamilu Rauf[7]

Abstract

This paper is proposing a novel technique that generates an unpredictable digit-size at every time of authentication. In this technique, neither the authentic user nor the hacker can have the prior knowledge of the digit-size not to think of the combinatorial (sequence or random order) of the anticipated keys. Indeed, this is simply referred to as Double-Blinded One-Time Password Key Generation (Double-Blinded-OTP). The technique harmonizes the methodology of Mutually Orthogonal Latin Squares (MOLS) and Resolvable Balanced Incomplete Block Designs (RBIBD). The uniqueness of the aforementioned designs make the proposed technique to be reliable and efficient to a large extent in mitigating the activities of hackers by protecting communications and the devices in Internet of Things (IoT).

Received: 10/02/2025, Accepted: 08/04/2025, Revised: 20/04/2025. * Corresponding author.
2015 *Mathematics Subject Classification.* 22E30, 26D10, 35P30, 47J10 & 58J05.
Keywords and phrases. Witten Laplacian, eigenvalues, Cheeger constant, Riemannian manifold & curvatures
[1&4]Department of Mathematics, Obafemi Awolowo University, Ile Ife 220005, Nigeria
[2,3,5&6]Department of Science and Engineering, Obafemi Awolowo University, Ile Ife, Nigeria
[7]Department of Mathematics, University of Ilorin, Ilorin, Nigeria
E-mails: ajsaka@oauife.edu.ng; sakajamiu@gmail.com
ORCID of the corresponding author: 0000-0003-0276-5579

1. Introduction and Preliminaries

Having realized that Single Factor Authentication (SFA) is prone to security threats, therefore in 2013, European Agency for Networking and Informative Security (ENISA) conducted a survey involving 100 professionals, in the year 2013 with the goals of identifying a strong and efficient authentication mechanisms to be used in financial services instead of the Single Factor Authentication (SFA) that was experiencing some weaknesses. As such, the survey led to recommendations that include the use of two-factor authentication, such as utilization of One-Time-Password (OTP) and tokens for all operations. Today, many mechanisms had been explored in OTP generations, but the fact remains that the hackers are equally intensifying efforts and successfully breaking into the mechanism behind those key generations. In addition, with the current usage of Internet of Things (IoT), web crimes have now become the concerns of most of multinational organizations and private individuals. Various sectors today are searching for sophisticated methods of providing efficient and sufficient security network or platform for their transactions in any public service. In order to attain and sustain such level of aforementioned security outfit, time-to-time update of security activities with strong monitoring are required. As such, different authentication levels due to peculiar situations and transactions could mitigate the activities of fraudsters.

Authentication is a verifiable process of affirming the originality of someone's assertion or claim. In the technological world, authentication provides access control for systems by checking to see if a user's details match with the exact information in a database before a clearance is granted for accessing an intended service. Generally, knowledge-based authentication (KBA), be it text-based or graphical passwords, is defined as an entity providing shareable secret information with the system for self authentication [7]. The use of One-Time Password (OTP) can serve as a supporting striker in beefing up security level of the existing passwords and it could be equally referred to as a second-level of authentication. [13] first suggested an OTP in early 1980s and this serves as a bedrock for other patented OTPs tokens that include; [9], [23] were presented.

[11] remarked that, there are other authentication mechanisms based on the user's physical unique identities such as biometrics Equally, token usage is another means of authentication system that depends on portable gadget [17]. Biometric leverages on biological identities of user, such as fingerprint, keystroke to identify and authenticate the intending users. Authentication with token requires the user to be in possession of the generator during the authentication period. Key-based authentication systems, such as Kerberos typically works on secret keys and stores by a machine [16] and [4].

Previous researches discouraged the use of single-factor authentication because the security level of single factor authentication is always at risk [5] and [3].

Meanwhile, due to the weakness observed in single factor [2] came up with multi-factors authentication mechanism that improves the security level against attacks because it asks users to provide more than one identifying entity.
In 2013, a survey involving 100 professionals was conducted by European Agency for Networking and Informative Security with the goals of identifying strong and efficient authentication mechanisms to be used in the financial services and also to determine the associated risks attached to them. To this effect, the survey outcome recommends the use of Electronic Identities and authentication methods for specific context and also the proportionality of method and risk [18]. The recommendations were based on two-factor authentication, utilization of tokens and passwords for all operations such as low risk, and to update and improve the knowledge and behaviours of both the customers and professionals in line with digital-finance security environments, digital-finance application and development [19].
Importantly, however, since Single Factor Authentication (SFA) is prone to security threat, researchers therefore suggested multi factor authentication (MFA) which involves the use of more levels of in dependency of security authentication of any user. For instance, the use of token to generates six digits at every operation. Hence, the need to present a double-blinded OTP generation technique to address such threats.

2. Review of Key Authentication in IoT

The Internet of Things (IoT) refers to the electrical devices that are connected and communicate over a network with aim of accessing and sharing a number of distinct dataset for different purposes. The aforementioned devices collect and generate required data from their domain using sensors and then transfer them to a central database through an appropriate channel. Meanwhile as technology continues to advance, every gadget around us generates data that are useful at every subset of IoT. Importantly, however, to secure the generated datasets becomes a serious concern for organizations that have keyed in into the use of IoT technology due to current insecurity in the use of internet. There was a survey that estimated that about 749 USD billion was spent on IoT in 2020. It is worthy to note that as devices connecting to internet increases, then the computing domain generates big data and this becomes very attractive and vulnerable to cyber crimes. It is therefore necessary and crucial to protect communications and shared devices on IoT against cyber crime.
[8], provided the current image of the internet of things authentication system and also a revealed the various authentication protocols in the literature. The study further revealed the robust protocol authentications that includes node capturing, replaying, password guessing, message forgery, sybil, brute forces, DoS, collision, chosen plaintext and so on with the aim that the aforementioned robust

protocol authentications be considered and analysed against potential attacks. [6] developed two types of authentication protocols for wireless sensor network with different security desires but the protocol was not able to provide the anticipated mutual authentication that harmonizes the challenges facing security and functionality. [14] also, presented a three factor user authentication protocol for wireless sensor network with the aim to eliminate the weaknesses and limitation observed in [6] protocols. To this effect, network simulator 3 (NS-3) was able to overcome the deficiency in the former protocol with a robust energy and efficiency for IoT applications. In addition, [20] and [14], proposed an improved scheme with resistance against spoofing attack and to ensure identity privacy using a multi factor authentication protocol by including one time password once the user's biometric information is authenticated by the gateway network while on internet of things. [15], studied the primitive features of polynomial and identified an important criterion for pseudo-randomness of ELCA cycles generation using linear rules. Also a new algorithms for cost effectiveness and flexibility was provided in the generation of one time password. To achieve harmonious authentication environment with IoT devices and their respective applications in line with the existing authentication schemes with appropriate security protocols which requires a two-factor authentication mechanism. As such, [21], therefore, presented a scaling, efficient and robust OTP scheme. Their technique was based on the principles of lightweight Identification with application of Elliptic Curve Cryptography scheme and Lamport's algorithm for OTP generation. They concluded that the proposed technique be adopted in real time IoT networks for two factor authentications on devices and for communications in IoT.

[22], examined the security issues relating to IoT devices currently being used via OTP codes sent through smart phones on how to keep devices safe away from intruders accessibility. The study concluded that the IoT device features such as a GSM module be used to automate requests via OTP codes to facilitate the authorization process.

In a review that focused on internet of things devices with respect to authentication techniques, [12], presented taxonomy cryptography that leverages on authentication system for IoT. Also, the advantages, limitation on the attacks related measure on the schemes were discussed. The study concluded that the schemes be modify to address a secure environment for IoT with respect to devices and users' architectures. The three-module system authentication was developed with time based OTP; keys exchange in unsecured communication system using a lightweight algorithm and encrypting data using SIT algorithm introduced by [10]. Thus, the proposed system combination of multi lightweight cryptographic resolution for a shared platform. [1] developed an algorithm to cater for the challenge facing the existing algorithms on lightweight cryptographic, such as NTSA,

which focuses on combining the high level of security for least of negative influence on running time with respect to speed and space. Applying One Time Pad (OTP) technique, the proposed system improves the security efficiency of NTSA.

3. Methodology

Here, mutually orthogonal latin squares, resolvable BIBDs and imbalance block designs are harmonized for the development of the proposed algorithms for keys generation.

3.1. **Mutually Orthogonal Latin squares (MOLS) Algorithm.** Let $M_{h\times h}(N_h)$ be set of h^2-matrices on $N_h = \{1, 2, \ldots, h\}$ for primes $h = 3, 5, 7, \ldots$. Let

$$Y_i = \begin{pmatrix} [p^i] \\ [p^{2i}] \\ [p^{3i}] \\ \cdots \\ \cdots \\ \cdots \\ [p^{(h-1)i}] \\ [p^{hi}] \end{pmatrix},\ Y_i^{-1} = \begin{pmatrix} [p^{-i}] \\ [p^{-2i}] \\ [p^{-3i}] \\ \cdots \\ \cdots \\ \cdots \\ [p^{-(h-1)i}] \\ [p^{-hi}] \end{pmatrix} \in M_{h\times h}(N_h) \text{ for } i = 1, 2, 3, ..., \frac{h-1}{2}$$

$$\text{where } < p >= \left\{p^{qi}\right\}_{q=1}^{h} = \left\{p, p^2, p^3, \cdots, p^{hi} = e\right\} \leq D_h \leq S_h \text{ with}$$

$[p^i], [p^{2i}], [p^{3i}], \cdots, \left[p^{(h-1)i}\right], \left[p^{hi}\right]$ being the least rows of the permutations $p^i, p^{2i}, p^{3i}, \cdots, p^{(h-1)i}, p^{hi}$ in their 2-row formats (similarly for Y_i^{-1} for $i = 1, 2, 3, ..., \frac{h-1}{2}$).

$$\text{Then, } L = \{Y_1, Y_1^{-1}, \cdots, Y_s, Y_s^{-1}\},\ s = \frac{h-1}{2} \text{ forms a set of MOLS.}$$

Proof. Consider a permutation $p \in S_h$ such that $\mid p \mid = h$ (i.e. $p^h = I$ (Identity permutation)), permutation $p = (1\ \ 2\ \ 3\ \ \ldots\ \ h)$ as a cycle. Let

$$Y_i = \begin{pmatrix} [p^i] \\ [p^{2i}] \\ [p^{3i}] \\ \cdots \\ \cdots \\ \cdots \\ [p^{(h-1)i}] \\ [p^{hi}] \end{pmatrix} \in M_{h\times h}(N_n) \tag{1}$$

for $i = 1, 2, 3, ..., \frac{h-1}{2}$ then

$$Y_i^{-1} = \begin{pmatrix} \left[p^{-i}\right] \\ \left[p^{-2i}\right] \\ \left[p^{-3i}\right] \\ \cdots \\ \cdots \\ \cdots \\ \left[p^{-(h-1)i}\right] \\ \left[p^{-hi}\right] \end{pmatrix} \in M_{h\times h}(N_n) \tag{2}$$

for $i = 1, 2, 3, ..., \frac{h-1}{2}$ where $M_{h\times h}(N_h)$ is the set of h^2-matrices over $N_h = \{1, 2, \ldots, h\}$ and $< p >= \left\{p^{qi}\right\}_{q=1}^{h} = \left\{p, p^2, p^3, \cdots, p^{hi} = e\right\} \leq D_h \leq S_h$ with $[p^i], \left[p^{2i}\right], \left[p^{3i}\right], \cdots, \left[p^{(h-1)i}\right], \left[p^{hi}\right]$ being the lower rows of the permutations $p^i, p^{2i}, p^{3i}, \cdots, p^{(h-1)i}, p^{hi}$ in their 2-row formats. Then X_i is obtained and similarly, X_i^{-1} for $i = 1, 2, 3, ..., \frac{h-1}{2}$.
Elements of the set

$$L = \{Y_1, Y_1^{-1}, \cdots, Y_s, Y_s^{-1}\}, \quad s = \frac{h-1}{2} \tag{3}$$

are mutually orthogonal Latin squares. □

The generation sample is shown in Figure 1.

Algorithm 1 Mutually Orthogonal Latin Square Generation

Require: Number of rows (n) and column (n)
Ensure: A set of $MOLS$ matrices

Initialize $MOLS$ **set**: Create an empty set to store the generated $MOLS$ matrices.
Generate Latin Squares:
for $i \leftarrow 1$ `to` n **do**
    `Generate a Latin Square` LS_i `of order` n`:`
        `Initialize` LS_i `as an` $n * n$ `matrix.`
        `Fill the first row of` LS_i `with numbers 1 to` n `in ascending order.`
        for $j \leftarrow 2$ to n do
            `Rotate the previous row of` LS_i `cyclically by one position to the left to generate the next row.`
        `Add` LS_i `to the` $MOLS$ `set.`
        end for
end for
Check Orthogonality:
    For each pair of Latin Squares LS_i and LS_j in the $MOLS$ set($i \neq j$):
        Check if the dot product of LS_i and LS_j equals 0 mod n.
            If the dot product is not zero, discard LS_i and LS_j and repeat step 2.
Repeat if Necessary:
    If the size of the $MOLS$ set is less than the required number of $MOLS$ matrices, return to step 2 and generate additional Latin Squares.
Output:
    Return the set of Mutually Orthogonal Latin Squares as the output of the algorithm.

3.2. **Resolvable Balanced Incomplete Block Designs (RBIBDs) Algorithm.**

Step 1:: Define a mapping $f : M_{h\times h}(N_h) \rightarrow M_{h\times h}(N^{h^2})$ and $f(X) = f\left((x_{m_j})\right) = \left(x_{m_j}^{(m-1)h+j}\right)$ for any $X = (x_{m_j}) \in M_{h\times h}(N_h)$ where $N^{h^2} = \{x^l \ : \ 1 \leq l \leq h^2, \ x \in N_h\}$.

Let $X = (x_{m_j}) = X_i, \ i = 1, 2, 3, ..., \frac{h-1}{2}$ so that $f(X_i) = f\left((x_{m_j})\right) = \left(x_{m_j}^{(m-1)h+j}\right) \ i = 1, 2, 3, ..., \frac{h-1}{2}$. Similarly, let $X^{-1} = (x'_{m_j}) = X_i^{-1}, \ i = 1, 2, 3, ..., \frac{h-1}{2}$ so that $f\left(X_i^{-1}\right) = f\left((x'_{m_j})\right) = \left(x'^{(m-1)h+j}_{m_j}\right) \ i = 1, 2, 3, ..., \frac{h-1}{2}$.

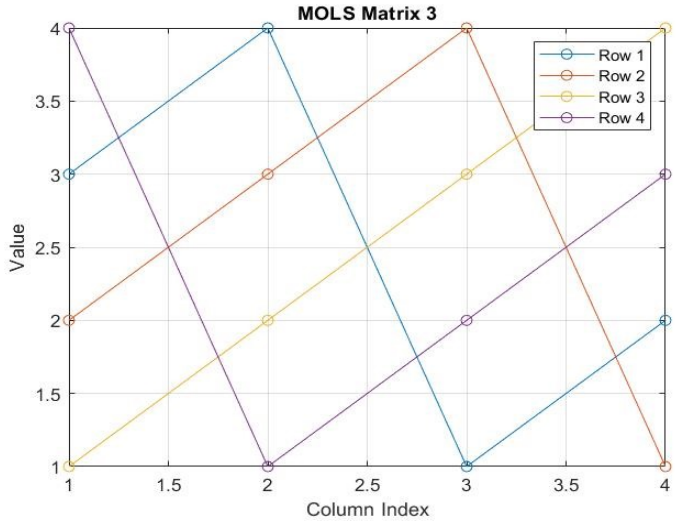


Figure 1: Matrix generation sample

Let $\Pi : f(X_i) = f\left((x_{m_j}\right) \in M_{h\times h}(N^{h^2}) \to Z \in M_{h\times h}(N_{h^2})$ be defined as $Z = \Pi\big(f(X_i)\big) = \Pi\big((x_{m_j})\big) = ((m-1)h+j) = (\pi_{mj}(r))\,,\ r = 1, 2, \cdots h.$ Then,

(4)

$$Y_i = \big[f(X_i)\big] = \begin{pmatrix} \pi_{1j}(1) & \pi_{2j}(1) & \cdots & \cdots & \pi_{(h-1)j}(1) & \pi_{hj}(1) \\ \pi_{1j}(2) & \pi_{2j}(2) & \cdots & \cdots & \pi_{(h-1)j}(2) & \pi_{hj}(2) \\ \pi_{1j}(3) & \pi_{2j}(3) & \cdots & \cdots & \pi_{(h-1)j}(3) & \pi_{hj}(3) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \pi_{1j}(h-1) & \pi_{2j}(h-1) & \cdots & \cdots & \pi_{(h-1)j}(h-1) & \pi_{hj}(h-1) \\ \pi_{1j}(h) & \pi_{2j}(h) & \cdots & \cdots & \pi_{(h-1)j}(h) & \pi_{hj}(h) \end{pmatrix}$$

for $i = 1, 2, 3, ..., \frac{h-1}{2}$ where $j = 1, \cdots, h$.
Similarly, the Y_i^{-1} correspond to X_i^{-1} and be found for $i = 1, 2, 3, ..., \frac{h-1}{2}$ using the similar approach. Hence, for any $n = 2h + 1$, where h is a natural number, RBIBD is

(5)
$$L = \{X_0, X_0^T, Y_1, Y_1^{-1}, \cdots Y_s^{-1}\}, \quad s = \frac{h-1}{2}$$

with complementary blocks obtained in step 2

Step 2:: The first two blocks are determined by $X_0 = ((m-1)h + j) =$

$$
\begin{pmatrix}
1 & 2 & \cdots & h-1 & h \\
h+1 & h+2 & \cdots & 2h-1 & 2h \\
2h+1 & 2h+2 & \cdots & 3h-1 & 3h \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
h(h-2)+1 & h(h-2)+2 & \cdots & h(h-2)+h-1 & h^2-h \\
h(h-1)+1 & h(h-1)+2 & \cdots & h^2-1 & h^2
\end{pmatrix} \tag{6}
$$

where the transpose of of X_0 denoted by X_0^T is given by $X_0^T = ((j-1)h + m) =$

$$
\begin{pmatrix}
1 & h+1 & \cdots & h(h-2)+1 & h(h-1)+1 \\
2 & h+2 & \cdots & h(h-2)+2 & h(h-1)+2 \\
3 & h+3 & \cdots & h(h-3)+3 & h(h-1)+3 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
h-1 & 2h-1 & \cdots & h(h-2)+h-1 & h^2-1 \\
h & 2h & \cdots & h^2-h & h^2
\end{pmatrix} \tag{7}
$$

Figure 2 represents the RBIBD construction sample.

Algorithm 2 RBIBD Construction

1: Initialize an empty RBIBD configuration matrix $RBIBDconfig$ of size $b * k$
2: Generate a set of b blocks, each containing k treatments represented by integers from 1 to v
3: For each block:
Ensure that each treatment appears exactly once within the block.
Ensure that each pair of treatments appears together exactly once in the entire configuration.
Ensure that each treatment appears in exactly r blocks, where r is the replication number.
Minimize the number of blocks, b
4: Ensure the resolvability of the RBIBD configuration:
Create a resolution matrix R, where each row represents a block and each column represents a pair of treatments.
Determine the number of times each pair of treatments appears together across all blocks and populate R.
Ensure that the resolution matrix R is a constant value (λ) for all pairs of treatments.
5: If the RBIBD configuration is not resolvable, adjust the parameters (b, k, v) and repeat the construction process until a resolvable configuration is obtained.
6: Output the constructed RBIBD configuration matrix $RBIBDconfig$.

3.3. **Imbalanced Block Designs Algorithm.** Here the results obtained in Section 3.2 are leveraged on via the algebraic function below to generate the imbalanced keys.

Let $M = (R_i)_{i=1}^{n} = (a_{ij})_{i,j=1}^{n} \in \mathcal{M}(\mathbb{N})$
or
$M = (R_i)_{i=1}^{n} \in \mathcal{M}_{n\times 1}(\mathbb{N})$
where $R_i = (a_{i1}, a_{i2}, \ldots, a_{in})$
f(subblock)=Token
$f(R_i) = R_i$
$f : \mathcal{M}_{n\times 1}(\mathbb{N}) \to \mathcal{M}_{n\times 1}(\mathbb{N})$
$f((a_{i1}, a_{i2}, \ldots, a_{in})) = (f(a_{i1}), f(a_{i2}), \ldots, f(a_{in}))$

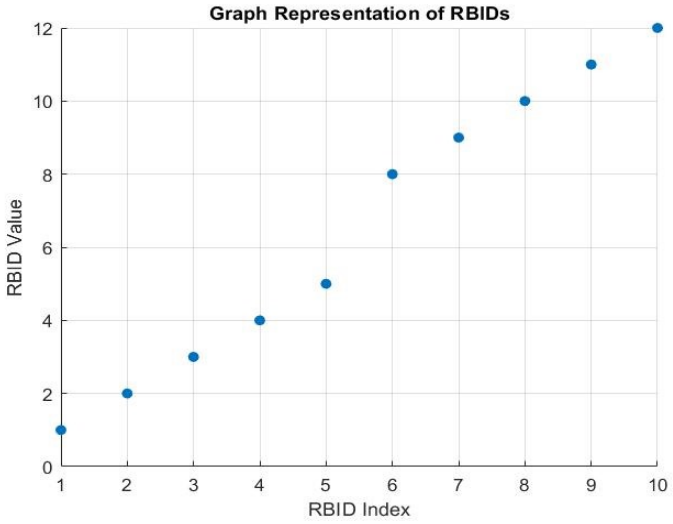


Figure 2: RBIBD configuration construction

where

$$f(a_{ij}) = \begin{cases} a_{ij} & \text{if } 1 \leq a_{ij} \leq 9 \\ x, y & \text{if } 1 \leq a_{ij} \leq 9 \\ & \quad 10 \leq a_{ij} \leq 99 \\ & \quad a_{ij} = x - 10 + y \\ & \quad a_{ij} = 10x + y \end{cases}$$

Algorithm 3 RBIBD Construction

Require: Mutually Orthogonal Latin Squares ($MOLS$) matrices and Resolvable Balanced Incomplete Block Designs ($RBIBD$) configuration.

Ensure: Double-blinded key for OTP generation.

1: Initialize an empty double-blinded key matrix $DBKey$ of size $n * n$, where n is the order of the MOLS.
2: For each row i in the MOLS matrices:
3: Select a random row r from the RBIBD configuration.
4: Concatenate the elements of row i from the MOLS with the corresponding elements from row r from the RBIBD configuration.
5: Add the concatenated row to the double-blinded key matrix $DBKey$.
6: Output the constructed double-blinded key matrix $DBKey$.

4. Double-Blinded OTP Key Generations

This section used the Algorithms 1 and 2 in Section 3 to generate the following unpredictable keys referred to as Double-Blinded OTP Keys:

1	2	3	4	5	.	.	.	.	.
6	7	8	9	1	0	.	.	.	.
1	1	1	2	1	3	1	4	1	5
4	8	1	2	1	6	2	5	.	.
4	7	1	5	1	8	2	1	.	.
1	6	1	1	1	6	2	1	.	.
2	7	1	2	1	7	2	2	.	.
3	8	1	3	1	8	2	3	.	.
4	9	1	4	1	9	2	4	.	.
5	1	0	1	5	2	0	2	5	.
5	9	1	3	1	7	2	1	.	.
1	1	0	1	4	1	8	2	2	.
2	6	1	5	1	9	2	3	.	.
3	7	1	1	2	0	2	4	.	.
1	6	1	7	1	8	1	9	2	0
2	8	1	4	2	0	2	1	.	.
3	9	1	5	1	6	2	2	.	.
4	1	0	1	1	1	7	2	3	.
5	6	1	2	1	8	2	4	.	.
1	7	1	3	1	9	2	5	.	.
2	1	2	2	2	3	2	4	2	5
5	8	1	1	1	9	2	2	.	.
1	9	1	2	2	0	2	3	.	.
2	1	0	1	3	1	6	2	4	.
3	6	1	4	1	7	2	5	.	.
3	1	0	1	2	1	9	2	1	.
4	6	1	3	2	0	2	2	.	.
5	7	1	4	1	6	2	3	.	.
1	8	1	5	1	7	2	4	.	.
2	9	1	1	1	8	2	5	.	.

Conclusion. The current usage of Internet of Things (IoT) has added to increase in web crimes. These crimes have now become the concerns of most multinational organizations and private individuals. Thus, Double-Blinded One-Time-Password keys were generated in block matrices. These block matrices are then leveraged on with imposition of some unique conditions which eventually creates

an Imbalanced Block Designs that finally generates an unpredictable digit-size as keys at every authentication level to the intending user as OTP. In this technique, neither the authentic user nor the hacker have the prior knowledge of the digit-size or the combinatorial sequence of the anticipated keys. Indeed, the technique is here referred to as Double-Blinded One-Time Password Key Generation (Double Blinded-OTP). The harmonization of MOLS and RBIBD makes the proposed technique unique, reliable and efficient to a large extent to mitigate the current web crimes in communications and devices usage in Internet of Things (IoT).

Acknowledgement: The authors are grateful to Obafemi Awolowo University and University of Ilorin for the supports they received during the compilation of this work.

Competing interests: The manuscript was read and approved by all the authors. They therefore declare that there is no conflicts of interest.

Funding: The Authors received no financial support for the research, authorship, and/or publication of this article.

References

[1] Al-Shareeda M. A., Manickam S. & Saare M. A. (2023). Enhancement of NTSA Secure Communication with One-Time Pad (OTP) in IoT. *Informatica*. **47**, 1-10.

[2] Bhivgade T., Bhusari M., Kuthe A., Jiddewar B. & Dubey P. (2014). Multi-factor Authentication in Banking Sector. International Journal of Computer Science and Information Technologies. **5** (2), 1185-1189.

[3] Brostoff S., Inglesant P. & Sasse M. A. (2010). Evaluating the usability and security of a graphical one-time PIN system. *In Proceedings of the 24th BCS Interaction Specialist Group Conference*. 88-97. British Computer Society.

[4] Callas J., Donnerhacke L., Finney H., Shaw D. & Thayer R. (2007). *Open PGP message format*. Technical Report (No. RFC 4880).

[5] Carullo G., Ferrucci F. & Sarro F. (2012). *Towards improving usability of authentication systems using smartphones for logical and physical resource access in a single sign-on environment*. In Information systems: crossroads for organization, management, accounting and engineering, Physica-Verlag HD. 145-153.

[6] Chang C. C. & Le H. D. (2016). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on Wireless Communications*. **15** (1), 357-366.

[7] Cranor L. F. & Garfinkel S. (2005). *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc., 175-197.

[8] El-hajj M., Fadlallah A., Chamoun M. & Serhrouchni A. (2019). A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors*. **2019**, 1-43.

[9] Kensuke S. (2011). *Authentication System, US8074075*

[10] Kollipara V. N. H., Kalakota S. K , Chamarthi S , Ramani S, Malik P. & Karuppiah M. (2023). Timestamp Based OTP and Enhanced RSA Key Exchange Scheme with SIT Encryption to Secure IoT Devices. *Journal of Cyber Security and Mobility*. **12** (1), 77-102.

[11] Jain A. K., Ross A. & Pankanti S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security*. **1** (2), 125-143.

[12] Labiod Y., Abdelaziz A. K., Ghoualmi N. & Ferrag M. A. (2019). *Authentication Scheme in Internet of Things: A Review*. Conference on Artificial Intelligence and Information Technology, ICA2IT. **19**, 181-190.

[13] Lamport L. (1981). Password Authentication with Insecure Communication. *In: Comm. ACM*. **24** (11), 770-772.

[14] Li X., Peng J., Niu J., Wu F., Liao J. & Choo K. R. (2017). A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. *IEEE Internet of Things Journal*. **2017**, 1-11.

[15] Mitra A., Kundu A., Chattopadhyay M. & Chattopadhyay S. (2017). A Cost-efficient One Time Password-based Authentication in Cloud Environment using Equal Length Cellular Automata. *Journal of Industrial Information Integration*. **1** (1),

[16] Neuman C., Hartman S., Yu T. & Raeburn K. (2005). it The Kerberos network authentication service (V5). Technical Report (No.RFC 4120).

[17] O'Gorman L. (2003). Comparing passwords, tokens, and biometrics for user Authentication. *Proceedings of the IEEE*. **91** (12), 2021-2040.

[18] Saka A. J., Adetina R. A. & Jaiyeola T. G. (2021). *A Simple Generalized Construction of Resolvable Balanced Incomplete Block Designs for k being a Prime for Block sizes. Advances in Mathematics: Scientific Journal*. **10** (6), 2767-2784.

[19] Saka A. J, Jaiyeola T. G., Adetona R. A. & Olurode K. A. (2022). A New Method of Construction of mutually Orthogonal Latin Squares of Prime Order. *Octagon Mathematical Magazine*. **30** (2), 900-917. ISSN: 2248-1893. (Romania).

[20] Tang A. S. W, Bong J. H, Teh Q. L., Sivalingam S., Chan S. S. Y, Khoo S. Y. & Naf T. M. (2021) Authentication of IoT device with the enhancement of One-time Password (OTP). *Journal of IT in Asia*. **9**, 29-40.

[21] Shivraj V. L., Rajan M. A., Singh M. & Balamuralidhar P. (2015). One Time Password Authentication Scheme based on Elliptic Curves for Internet of Things (IoT). *The 5th IEEE National Symposium on Information Technology: Towards Smart World*. **2015**, 1-6.

[22] Zendrato M., Zarlis M., Efendi S., Barus E. S., & Fahmi S. H. (2019). Increase Security of IoT Devices Using Multiple One Time Password. The International Conference on Computer Science and Applied Mathematic. *IOP Conf. Series: Journal of Physics: Conf. Series*. **1255** (2019) 012030, 1-6.

[23] Zhou L. & HuaZhang Y. (2012). :*One time password generating method and apparatus*, US8184872.