TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 19, No. 6, December 2021, pp. 1872~1883
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v19i6.21665

A secured data transform-and-transfer algorithm for energy internet-of-things applications

Abbas M. Al-Ghaili[1], Hairoladenan Kasim[2], Naif Mohammed Al-Hada[3]
[1]Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Selangor, Malaysia
[2]College of Computing & Informatics, Universiti Tenaga Nasional, Selangor, Malaysia
[3]Shandong Key Laboratory of Biophysics, Institute of Biophysics, Dezhou University, Dezhou, China

Article Info

Article history:

Received Aug 27, 2020
Revised Oct 9, 2021
Accepted Oct 18, 2021

Keywords:

Digital transformation
Digitization
Energy internet of things
Security

ABSTRACT

Digital transformation (DT) is one of the key technologies with effective impacts on many traditional processes towards a digital world. DT influences the way other digital services behave. Hence, there is a need to consider DT-related processes carefully specifically while designing phase. DT contributes to many services. It can, for example, contribute to implement security tasks applied to digital contents and therefore can be applied to change contents being secured. One of the transformation ways applied in security is to consider the way those digital contents are being stored or transferred. This paper proposes a DT algorithm (DTA) for energy internet-of-things (EIOT) contents. DTA consists of two steps, to convert original contents to another digital form and to transfer that form utilizing IOT. This paper utilizes DT in term of security. EIOT contents are converted to increase security. It is aimed to transfer EIOT contents to destination safely and efficiently. Thus, EIOT contents are transformed first to hide original contents. To make sure that the transferring process is done safely, DTA is evaluated in terms of efficiency, accuracy, and robustness. Results confirm that DTA is efficient, accurate, and robust against loss of bits caused by transferring.

Corresponding Author:

Abbas M. Al-Ghaili
Institute of Informatics and Computing in Energy
Universiti Tenaga Nasional
43000 Kajang, Selangor, Malaysia
Email: abbas@uniten.edu.my

1. INTRODUCTION

Digital transformation (DT) simply refers to change a form of data contents to another utilizing the conception of digitization [1] or capability of a process to be transform in a digital way to come up with a successful and effective result [2]. It is also defined as the state of two digital forms of data contents being changing digitally. One of these examples is the cloud computing. There are however several examples e.g., binary conversion, software development, and so on. Due to importance of DT and being developed rapidly, there have many fields utilized its impact and features. DT can influence the performance of such processes to enable them for rapidly developed results. The behavior of processes has been effectively enhanced [3]-[6].

DT has contributed in enhancing performance of processes for different areas and applications [7]-[10]. For example, DT has an obvious impact to logical systems and also industry world such as transistors development reaching digital computers development [11]. Furthermore, DT has accelerated the change of the Internet's development. Therefore, many other associated services and processes get effected and enhanced.

As for example, high demand(s) on Internet-related equipment and operations at different layers and conceptions starting from information technology [12]. This change has led to introduce new Internet-utilized era specifically for e-commerce and smart internet-based processes [13], [14].

DT has contributed to establish a number of fields such as digital information, media and technology [15], video processing, cognitive systems, security [16], smart systems, and Industry 4.0 [17] and other fields such as information system in digital business problems [18]. Digital information was first time really introduced and used in as a code in 1941 [19]. The programmable computer to use binary coding has been designed. In that design, thousands of transistors have been included for the selected microprocessor as an example of digital information and transformation used for digital computers.

In addition, in media and technology, DT has helped enhancing related services and functions that can be implemented in a semi- real-time behavior utilizing digitization technologies to exploit hardware sensors achieving a digital transformation concept as in virtual reality (VR) to contribute to industrial production services [20]. Similarly, video data processing has enhanced many other related services and products for several sectors [21] e.g., industry, communication, health, security systems, unmanned aerial vehicles (UAV), and 3D frames sequences. For these applications, a huge amount of data contents is processed and therefore video processing is considered important for DT. Not far from this sector, audio and image codecs [22] is one of the key sectors that has been exploited DT to enhance its services to enhance listening and recording services for a better digital era. Sometimes, audio codecs related processes will be integrated in hardware [23] utilizing the conception of digital transformation. Research studies have considered DT-utilized business and e-markets in many sectors [24], [25]. One of these sectors is banks whereas a research study proposing a method to utilize digital technologies that transform banks-related classical processes into digital ones is discussed in [26].

DT has contributed to many sectors in our digital life areas in smart ways. One of these sectors is the smart energy. That includes energy smart management for all energy-related sources. Of the effective energy smart management way is to increase the security of energy-related systems e.g., smart meters, and data-driven services. Security starting from collection of energy-related data sources (plaintext), to performing encryption scheme, to performing analysis of digital image process for security purposes, to performing actionable instructions towards hardware equipment e.g., automatic secure gates and biometrics security authentication devices. This research study concerns the conversion of original data contents to another types of data format. The second concern of this paper is to propose a mechanism that changes the way the data contents are stored by. This paper is organized as follows: in section 2, the proposed concept of digital transformation framework will be explained. Section 3 presents the proposed digital transformation algorithm (DTA) of EIOT contents. Results and discussion are presented in section 4. Conclusion is drawn in section 5.

2. THE PROPOSED CONCEPT OF DIGITAL TRANSFORMATION FRAMEWORK

2.1. Overview

This proposed framework shows how energy related contents can be exploited by internet-of-things (IoT) applications. Energy IoT (EIoT) contents are considered for the aim of security. EIoT contents might be images or text data types which they will be converted to another data form (i.e., transformed) first and then transferred digitally. Then, it is used in its encrypted form by many smart EIoT-related applications. The proposed framework consists of two main steps as illustrated in Figure 1.

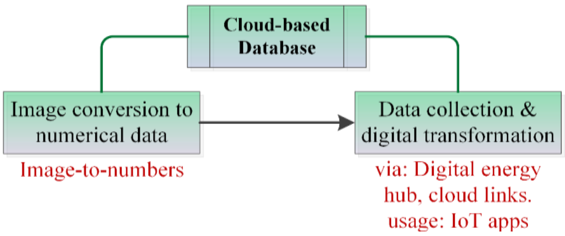
Cloud-based Database
Image conversion to numerical data
Image-to-numbers
Data collection & digital transformation
via: Digital energy hub, cloud links.
usage: IoT apps

Figure 1. Digital image transformation for IOT applications – a proposed framework

2.2. Data conversion to a 1D integer array

The first step of the proposed framework converts the image into numbers. The aim is to use those numbers for encryption purposes. The flowchart of this step is depicted in Figure 2. As mentioned in this figure, there are two processes marked in red-colored signs. In the first one, the image-data will be the input (image #i) in order to detect its edges, for example. Those edges will be distinctly highlighted. Then, the edges detected image (I_{ED}) will be produced. A series of image conversions will be applied on image #i to produce I_{ED}. The second process will represent the I_{ED} to a 1D array by using a series of mathematical operations on I_{ED}. To do so successfully, pixels' intensities (i.e., positive integer values corresponding to image colors) of I_{ED} will be extracted. Those integer numbers will be converted to unknown numbers. They are ordered as a 1D alphanumeric array.

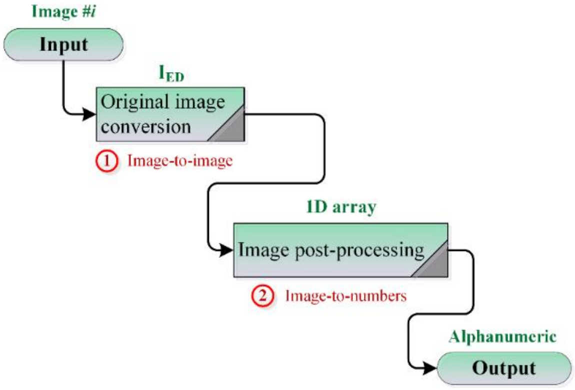

Figure 2. Block-diagram of image-data conversion to a mathematical array

2.3. Digital transformation for collected data

This step consists of three processes as illustrated in Figure 3. In this figure, there are three processes marked in blue, brown, and green colored boxes. The first process applies an encryption scheme to values of I_{ED} image (or EIOT contents) to produce an encrypted value. In the second process, the encrypted values will be sent to digital transformation storage. After that, they will be transferred via a cloud-based technique to a third party. The third process receives transferred information from cloud storage. The encrypted information is processed using IOT application(s). This information in its encrypted form could be used as a smart key to access a digital asset or used for smart services after they have been verified.

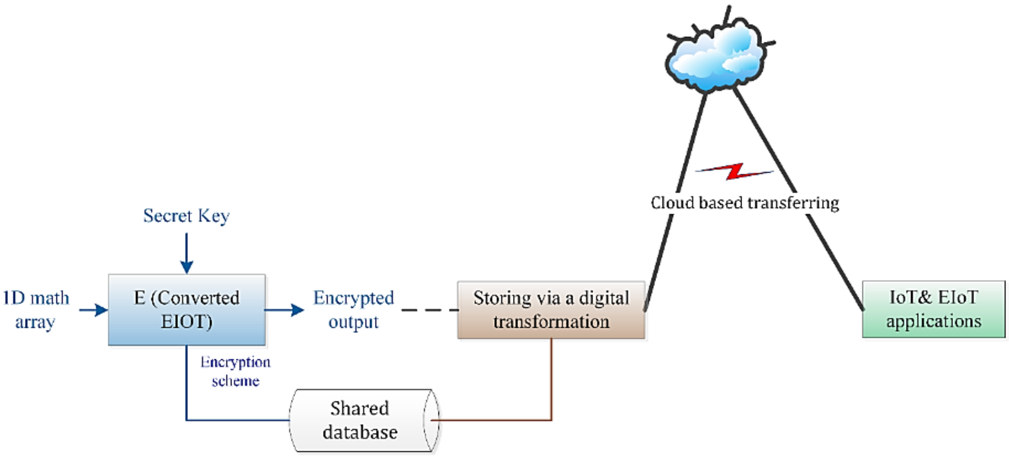

Figure 3. Digital transformation block-diagram

3. THE PROPOSED DIGITAL TRANSFORMATION ALGORITHM (DTA) OF ENERGY INTERNET-OF-THINGS (EIOT) CONTENTS

3.1. Overview

Given is an un-encrypted data content, it is the aim to create a safe and secure environment while transformation of energy related data for energy security purposes. In this sub-section, the conception the digital transformation is performed for energy IOT (EIOT) will be discussed. EIOT contents might include data related to site, data related to devices and equipment, or data related to users and accounts involved with energy systems. These data are utilized by other related parties at destination(s). It is needed to send them to the destination by utilizing IOT medium e.g., cloud-based computing devices and systems. It is necessary to keep such data private and secure. Therefore, data related to energy systems to be transferred to the destination using IOT technology is considered EIOT contents. Thus, transformation of these contents needs to be carefully and securely performed. Security of EIOT contents is highly considered. Thus, it is essential to change its raw form and convert it to unknown forms. Additionally, transferring these contents has to be verily done to make sure contents reach destination(s) efficiently.

3.2. Proposed DTA flowchart

The proposed digital transformation algorithm (DTA) consists of two parts carried out in a securely performed manner. The first part is EIOT contents conversion and the second part is EIOT contents transferring. The first part concerns conversion of EIOT contents to another form by implementing encryption schemes while the second part considers the transferring of EIOT contents between the sender and receiver parties. The proposed DTA flowchart is shown in Figure 4. In this figure, there are three rounds of encryption using different schemes for conversion purposes of EIOT contents. These three rounds are in detail explained later. Once, the verification procedures are implemented before any data transferring has taken a place.

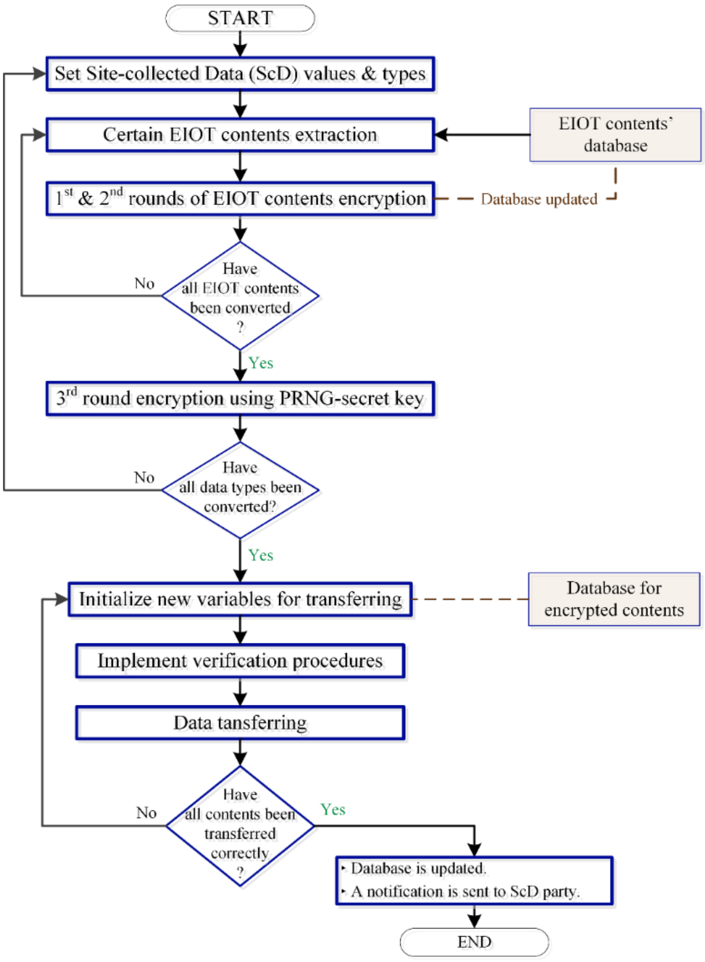
START
Set Site-collected Data (ScD) values & types
Certain EIOT contents extraction
EIOT contents' database
1st & 2nd rounds of EIOT contents encryption
Database updated
Have all EIOT contents been converted ?
No
Yes
3rd round encryption using PRNG-secret key
Have all data types been converted?
No
Yes
Initialize new variables for transferring
Database for encrypted contents
Implement verification procedures
Data tansferring
Have all contents been transferred correctly ?
No
Yes
Database is updated.
A notification is sent to ScD party.
END

Figure 4. The proposed DTA flowchart

3.3. The proposed EIOT contents' conversion algorithm (EICA)

EICA aims to change the known form of EIOT contents to an unknown form of data. To do so, conversion procedures of the original contents need to be implemented first on EIOT contents. Prior to the conversion procedure, there are few pre-processes performed to initialize related variables e.g., types of data and data preparation.

3.3.1. Set site-collected data (ScD) values & types

In this step, the site being used will be assigned a certain value. This value is set to point out that its site is considered for the conversion process. Meaning, there are many sites from which data is collected. Each time, only one site is processed. This is mathematically represented in (1).

$$S_{ScD} = S_i | i = 1,2, \dots n \quad (1)$$

Where,

– S_{ScD} is the site to be selected
– S_i is the i^{th} site already selected
– i is the assigned value to point out that the i^{th} ScD is currently occupied and data is being collected from
– n is total number of sites.

Another issue is that, there are two types of data considered which are images and texts data types. Sometimes, it is aimed to process one of two data types either an image or a text file. The formula applied to detect either an image or a text data type is selected is mathematically represented in (2).

$$T_D = \begin{cases} img_{S_i}, & i_g \neq \text{null AND } i_x = \text{null} \\ txt_{S_i}, & i_x \neq \text{null AND } i_g = \text{null} \end{cases} \quad (2)$$

Where,

– T_D is the data type file is selected
– i_g is an image indicator; if this value is true; then T_D is an image collected from S_i, img_{S_i}
– i_x is a text indicator; if this value is true; then T_D is a text data collected from S_i, txt_{S_i}.

As noticeable obvious from this equation, at each time, a single data type is processed.
The pseudocode of both procedures (mentioned in (1) and (2)) will be provided in Algorithm 1.

Algorithm 1. ScD function to set values and data-types

```
main ()
  For i =1 to n
    do {
     $S_{ScD}$=$S_i$;
     ScD←i;
     } while(!($S_i$==Null));
    break();
  End For
  If ($S_i$⊃{{image|text}})
    {
    $T_D$=call select(image, text);
    call conversion($T_D$); }
  End If
End main()
```

Once the site has been set to value "1", that means the related site (S_{ScD}=S_i) is considered. The next step is to select one type of data to be processed by converting original contents to another form of a non-understandable form by using two functions namely select *()* and conversion*()* for data-type, i.e., T_D, selection and conversion, respectively. The select function receives two inputs and returns one output. Below is a graphical representation of the steps mentioned in the pseudocode for a more clarification purpose as shown in Figure 5. As can be seen in this figure, after values are set in regarding ScD, the type of data is selected before the data is sent to conversion. There are several steps applied to data in order to convert raw contents, as can be discussed in the following sub-sections.

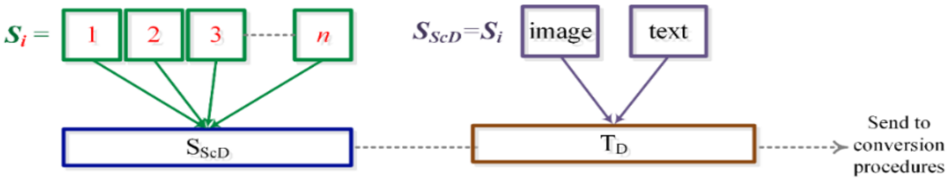

Figure 5. A graphical representation of Algorithm 1 related procedure

3.3.2. Certain EIOT content extraction

In this sub-section, data is divided into two parts one of which will go for the conversion procedure first while the other part will be later converted using a different conversion procedure so that can increase security of EIOT contents. In order to do, contents of such data will be put in two parts in relation to T_D, as formulated in (3) and (4).

$$c_1 = e_1(T_D) \tag{3}$$

$$c_2 = e_2(T_D) \tag{4}$$

Where,
- c_1 represents the first part of EIOT contents
- e_1 is the extraction function applied on T_D to extract certain EIOT contents for the first conversion procedure
- T_D is the data type used
- c_2 represents the second part of EIOT contents
- e_2 is the extraction function applied on T_D to extract certain EIOT contents for the second conversion procedure.

As for the extracted contents, for the first conversion procedure, the input will be c_1 while c_2 is the input for another conversion procedure. There should have been two different conversion procedures applied to c_1 and c_2, discussed in the following sub-sections.

3.3.3. Data conversion using encryption

In this step, it is an encryption scheme applied to the first part of EIOT contents either an image data or text data. The formula used in this step is defined in (5).

$$C_{1_D} = E(c_1) \tag{5}$$

Where,
- C_{1_D} is the data conversion procedure applied to the first part of EIOT contents
- $E(c_1)$ is the encryption of EIOT contents defined in (3)

As then, (5) is re-written as in (6).

$$C_{1_D} = E\big(e_1(T_D)\big) \tag{6}$$

As for a substitution to determine the type of data is been encrypted, (6) is re-formulated in (7).

$$C_{1_D} = E\left(e_1\begin{pmatrix} img_{S_i},\ i_g \neq \text{null AND } i_x = \text{null} \\ txt_{S_i},\ i_x \neq \text{null AND } i_g = \text{null}\end{pmatrix}\right) \tag{7}$$

The proposed encryption scheme applied to c_1 in which its data type is mentioned in (7) is shown in Figure 6.

The output is stored in a form of binary numbers as formulated in (8).

$$C_{1_D} = bin\left(E\left(c_1, k_{c_1}\right)\right) \tag{8}$$

Where,
- $bin(\dots)$ is the binary conversion function applied to the encrypted value
- $E(\dots)$ is the encrypted function applied to both EIOT contents, c_1, and the related secret key, k_{c_1}.

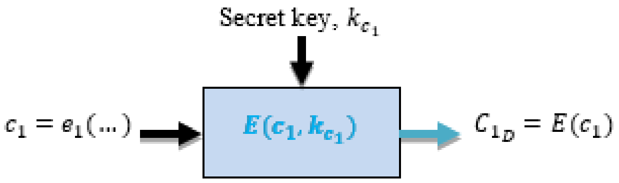

Figure 6. Conversion procedure of first part of EIOT contents, i.e., c1

3.3.4. Encryption using three-valued logic (3VL)

Certain EIOT contents that have not been converted by the first procedure, i.e., c_2, will be processed in this part. Specifically, c_2 will be encrypted using a different encryption scheme. Firstly, those EIOT contents will be divided into blocks of data as in (9). An extended mathematical representation is defined in (10).

$$B[\dots] = \{\{block_i;\ i = 1,2,\dots m\} \tag{9}$$

$$B[\dots] = \{\{block_1, block_2, \dots block_m\} \qquad (10)$$

Secondly, each block will be converted to binary numbers. Thirdly, each binary block will be converted into three-valued logic (3VL) numbers. Each third binary value exists in binary blocks will be replaced by a trinary <*xy*> value. Finally, an encryption scheme is applied to 3VL blocks, one-by-one, using (11).

$$C_{2_D} = E\big(\{\{block_1, block_2, \dots block_m\}, k_{c_2}\big) \qquad (11)$$

This proposed procedure is explained in a more detailed way as illustrated in Figure 7.

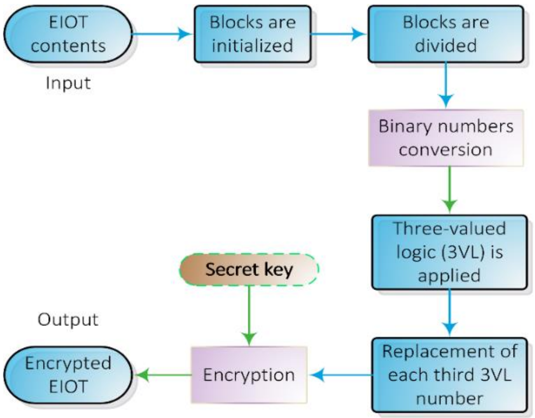

Figure 7. A graphical representation of the proposed 3VL block-diagram

3.3.5. Encryption scheme using PRNG-based complicated secret key

In this step, EIOT contents encrypted earlier will be encrypted in two subsequent schemes. So far as discussed earlier, EIOT contents consist of c_1 and c_2. Each scheme will be fed by a distinctively different secret key. A pseudorandom number generator (PRNG) is used to generate a complex secret key with long size. The proposed block-diagram of this encryption scheme is shown in Figure 8.

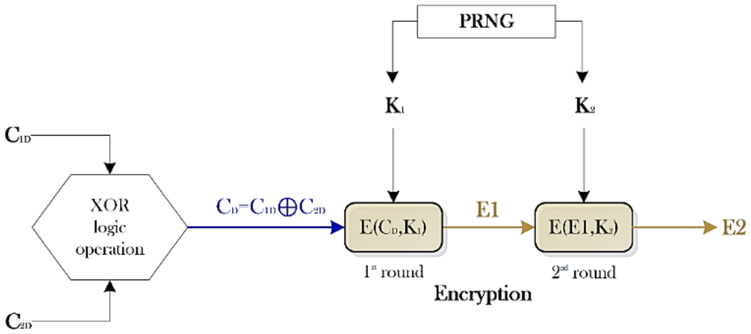

Figure 8. Encryption scheme using PRNG for secret key(s)

In this figure, there are two rounds of encryption using different secret keys. Before any encryption scheme is done, a logical XOR operation is performed on previously encrypted EIOT contents, which are C_{1_D} and C_{2_D}. The logical formula applied to perform XOR operation is defined in (12).

$$C_D = C_{1_D} \oplus C_{2_D} \qquad (12)$$

Before the XOR operation is performed, a formalization process to adjust length of both C_{1_D} and C_{2_D} in relation to binary numbers is done by using (13) and (14).

$$C_{1_D} = f_{form}(\hat{C}_{1_D}) \qquad (13)$$

$$C_{2_D} = f_{form}(\hat{C}_{2_D}) \tag{14}$$

Where:
- $\hat{C}_{1_D}$ and $\hat{C}_{2_D}$ are series of binary number for the converted first and second parts of EIOT contents before they are formalized, respectively
- $f_{form}(\dots)$ is the formalization function
- C_{1_D} and C_{2_D} are series of binary number for the converted first and second parts of EIOT contents after they are formalized, respectively.

For encryption, there have been two rounds of encryption implemented using two different secret keys with the help of PRNG. For this purpose, there are two procedures implemented to do encryption using (15) and (16). Furthermore, two PRNG-based secret key generation procedures are performed using (17) and (18).

$$E1 = E(C_D, K_1) \tag{15}$$

$$E2 = E(E1, K_2) \tag{16}$$

$$K1 = f_1(Xn) \tag{17}$$

$$K2 = f_2(Xn) \tag{18}$$

Where $f_1(Xn)$ and $f_2(Xn)$ are functions of PRNG-based definition(s) used to generate K1 and K2, respectively. They are mathematically defined in (19) and (20).

$$f_1(Xn) = f_1((a_1 X_n + c)\ mod\ m) \tag{19}$$

$$f_2(Xn) = f_2((a_2 X_n + c)\ mod\ m) \tag{20}$$

3.4. The proposed EIOT contents' transferring algorithm (EITA)

Transferring EIOT contents is not a simple straightforward task. This step performs several procedural verifications to make sure the security issue is considered, which are as follows:

3.4.1. Time-based verification (TbV)

This procedure of verification is performed in a scheduling manner using a time-intervals mechanism. At each interval of time, the TbV runs a group of procedures to verify the followings:
- is number of transferred blocks true? $\mathrm{E}_{\mathrm{n}_{\mathrm{block}}}$ → Efficiency analysis
- have all transferred blocks of data been received accurately and correctly? → Accuracy measurement analysis
- how many blocks were defeated? → Accuracy measurement analysis
- how many blocks were received? → Robustness against unauthorized actions and attacks → security detection rate

3.4.2. Error-free verification (EFV)

EFV makes sure that there is error-free while transferring in terms of block-bits loss. If there is a block's bit lost, it is considered that EFV=False. This is mathematically defined in (21).

$$EFV = \begin{cases} True,\ B_{block_i} = !\,(NULL) \\ False,\ B_{block_i} = NULL \end{cases} \tag{21}$$

If there is a possibility that a single bit, B, that belongs to a block of data $block_i$ is lost, its *returned* value to the variable B_{block_i} becomes Zero or as defined in (21) is a $NULL$, therefore, there is an error and it means no error-free; thus, EFV must be $False$, and vice versa. To say there is an error, it is important to check if there is a loss in blocks' bits or not. To make sure for such a case; it is important to check these conditions: If *loss* of B_{block_i} at least contains one bit, $B_{block_i} = NULL$ and If *loss* of B_{block_i} equals to 0 bit, $B_{block_i}!\,(NULL)$. This is done using (22).

$$B_{block_i} = \begin{cases} !\,(NULL),\ l_{B_{block_i}} < 1 \\ \quad NULL,\ l_{B_{block_i}} \geq 1 \end{cases} \tag{22}$$

If only 1-bit is lost, it is considered: EFV includes an error (i.e., $l_{B_{block_i}} = 1$) and that could affect efficiency of the proposed DTA. But, if more than 1-bit is lost, it is considered EFV includes several errors ($l_{B_{block_i}} > 1$) and a defeated block exists which may affect accuracy of DTA.

3.4.3. Error correction code (ECC)

Once a block has been transferred, it is necessary to make sure that there is no error and no need to correct it. This code equals to one of two logical values; either 0 or 1, as defined in (23).

$$ECC = \begin{cases} 0, & EFV = True \\ 1, & EFV = False \end{cases} \tag{23}$$

Iff $ECC = 0$, then that means there is no error and $EFV = True$. Thus, this case is suitable to transfer further blocks. But, Iff $ECC = 1$ then an error exists and cannot transfer EIOT contents.

3.4.4. Confirmation notification of transfer (CNT)

If ECC==Zero, a notification to confirm suitability of transferring is sent to the sender party. The proposed pseudocode to briefly explain how the CNT is implemented is provided in Algorithm 2:

Algorithm 2: CNT process

```
If(ECC==0)
{
  CNT= True;
  Transferring = enabled;
}
End If
```

4. RESULTS AND DISCUSSION

In this section, there are three evaluation types performed which are: efficiency, accuracy, robustness, and computational complexity of the proposed DTA.

4.1. DTA Efficiency

The proposed DTA considered the quantity being transformed at firstly. In this type of evaluation, the number of blocks has been transformed will be calculated. If the number of blocks denoted by: n_{block} in a relation with $block_i$ is as maximum as n; that means it is efficient in terms of quantity. To do so, (24) is used.

$$E_{n_{block}} = \frac{f\left(block_{\ddot{T}}\right)}{block_i}\% \tag{24}$$

Where,

- $E_{n_{block}}$ denotes the efficiency percentage
- $f(block_{\ddot{T}})$ denotes a sum function that calculates how many blocks have been transformed ($block_{\ddot{T}}$), successfully
- $\ddot{T}$ denotes a block that has been transformed successfully
- $block_i$ denotes the total number of blocks before the transformation function is implemented.

There are 118 samples to which DTA has been applied. Length (size) of each sample belongs to one of two lengths. Meaning, there have been two lengths each sample belongs to selected. One length has been set to 25 blocks and the other one has been set to 37 blocks. There are then two experiments carried out to which (24) is applied. Samples used in these experiments are summarized in Table 1. Once, (24) has been applied on experiments mentioned in Table 1, results obtained then are shown in Figure 9. In this figure, 1712 and 1739 successfully transformed blocks are obtained for experiments 1 and 2 with efficiency percentages equal to 97.8 and 97.9%, respectively.

Table 1. Samples and types of samples

Experiment	#samples/ experiment	Length	Type
1	70	25	Text
2	48	37	Image, text

4.2. DTA accuracy based on bits of blocks B_{blocks}

In this evaluation, bits of blocks are considered. The number of bits has not been successfully transformed is obtained. This number of bits will affect the accuracy of the proposed DTA. In order to perform this measurement, there are two mathematical procedures implemented, which are as follows: first, while there are two experiments consisting of 70 and 48 samples with 25 and 37 blocks, respectively. Amongst these two experiments, 1712 and 1739 blocks were successfully transformed. Unsuccessful transformed blocks are mentioned in Table 2.

Second, the received transformed no. of bits is to be 883456. But, the accurate number of bits has been received is 881702 bits. That means a number of bits has been lost and that will affect the accuracy of DTA. Percentages of successful transformed bits for two experiments as well as averaged accuracy of the proposed DTA will be shown in Figure 10. As can be seen in this figure, the accuracy of DTA is affected not only by transformed blocks but by bits being lost. Thus, the DTA accuracy has been reduced to 97.67% due to loss a number of bits while transformation.

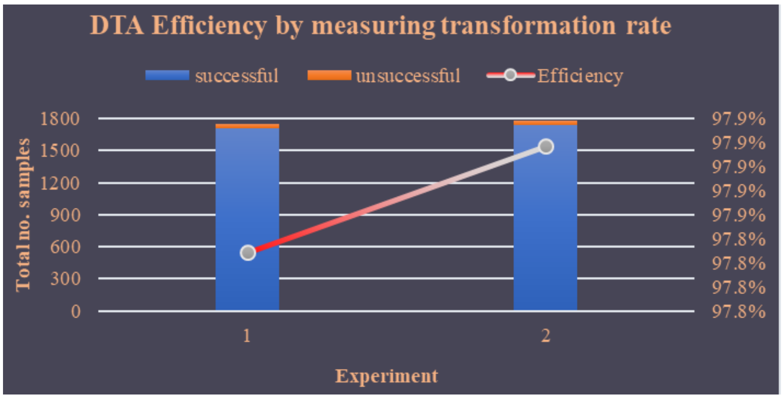

Figure 9. Evaluation of DTA in terms of efficiency and successful transformation rate

Table 2. Unsuccessful vs. successful transformed blocks

Experiment	Status of transformation	#Blocks	Bits/block	Total no. bits
1	Unsuccessful	1750-1712 = 38	256	256*38=9728
	Successful	1712		256*1712=438272
2	Unsuccessful	1776-1739 = 37		256*37=9472
	Successful	1739		256*1739=445184
Total	Unsuccessful	38+37=75		19200
	Successful	3451		883456

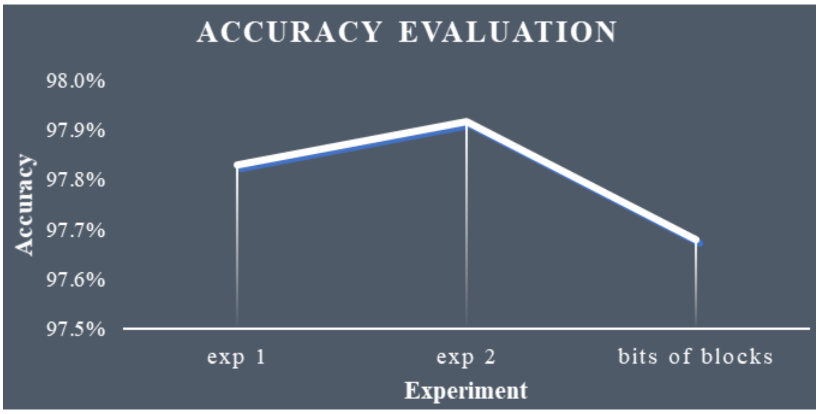

Figure 10. DTA's accuracy evaluation

4.3. Robustness of DTA

As discussed above, accuracy of DTA has been reduced due to several issues. One of these issues is that a number of bits from several blocks have not been received. Some blocks have been defeated totally and some others have partially received. All these issues have affected the performance of the DTA. Nevertheless, the proposed DTA is still considered robust against many factors that affect it performance. While the reduction in accuracy has been slightly occurred, the DTA accuracy is considered high and the unsuccessful transformation rate was ≈ 0.01%.

4.4. Computation complexity of DTA

There is one for loop i=1 to n, there are n times of repetitions of executable commands or instructions plus one instruction. That means, the computation complexity will be given in (25).

$$C\_CXTY = n \tag{25}$$

Where the C_CXTY and n represent the computational complexity of the proposed algorithm and the obtained value of $\_CXTY$, respectively.

5. CONCLUSION

This paper has proposed a digital transformation algorithm (DTA) in order to perform a transformation-based process applied to Energy related contents utilized IOT technology in which data is collected from a site. The DTA includes an EIOT-contents' conversion algorithm (EICA) and EIOT-contents' transferring algorithm (EITA) to implement a conversion process applied to EIOT contents first before the transferring is done by EITA. The DTA has been evaluated in terms of efficiency, accuracy, and robustness. The DTA has confirmed it is efficient in transferring EIOT contents with averaged percentage equals to 97.8%. The accuracy obtained from experiments has been found 97.7%. Obtained results have confirmed the robustness of the proposed DTA with an unsuccessful rate ≈0.0%. The proposed DTA has an impactful role on traditional processes in terms of security and computation time. The proposed DTA has helped solve the successful transferring rate with a very low loss-in-bits compared to other traditional algorithms. The novelty of the proposed DTA is that it helps reduce the loss-in-bits while transferring.

ACKNOWLEDGEMENT

This research is funded by Universiti Tenaga Nasional (UNITEN) with Grant Code: (RJO10517844/007) and Grant Code: (J510050002/2021048).

REFERENCES

[1] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 36, no. 4, 2019, doi: 10.1016/j.giq.2019.06.002.

[2] P. C. Verhoef *et al.*, "Digital transformation: A multidisciplinary reflection and research agenda," *Journal of Business Research*, vol. 122, pp. 889-901, 2021, doi: 10.1016/j.jbusres.2019.09.022.

[3] M. F. Ivanovici and M. Pană, "From Culture to Smart Culture. How Digital Transformations Enhance Citizens' Well-Being Through Better Cultural Accessibility and Inclusion," *IEEE Access*, vol. 8, pp. 37988-38000, 2020, doi: 10.1109/ACCESS.2020.2975542.

[4] A. Miklosik and N. Evans, "Impact of Big Data and Machine Learning on Digital Transformation in Marketing: A Literature Review," *IEEE Access*, vol. 8, pp. 101284-101292, 2020, doi: 10.1109/ACCESS.2020.2998754.

[5] F. Zaoui and N. Souissi, "Roadmap for digital transformation: A literature review," *Procedia Computer Science*, vol. 175, pp. 621-628, 2020, doi: 10.1016/j.procs.2020.07.090.

[6] J. Wu, S. Guo, J. Li, and D. Zeng, "Big Data Meet Green Challenges: Greening Big Data," *IEEE Systems Journal*, vol. 10, no. 3, pp. 873-887, 2016, doi: 10.1109/JSYST.2016.2550538.

[7] S. Singh, M. Sharma, and S. Dhir, "Modeling the effects of digital transformation in Indian manufacturing industry," *Technology in Society*, vol. 67, 2021, doi: 10.1016/j.techsoc.2021.101763.

[8] L. Tangi, M. Janssen, M. Benedetti, and G. Noci, "Digital government transformation: A structural equation modelling analysis of driving and impeding factors," *International Journal of Information Management*, vol. 60, 2021, doi: 10.1016/j.ijinfomgt.2021.102356.

[9] M. Massaro, "Digital transformation in the healthcare sector through blockchain technology. Insights from academic research and business developments," *Technovation*, 2021, doi: 10.1016/j.technovation.2021.102386.

[10] Z. Yang, J. Chang, L. Huang, and A. Mardani, "Digital transformation solutions of entrepreneurial SMEs based on an information error-driven T-spherical fuzzy cloud algorithm," *International Journal of Information Management*, 2021, doi: 10.1016/j.ijinfomgt.2021.102384.

[11] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and Communications Technologies for Sustainable Development Goals: State-of-the-Art, Needs and Perspectives," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2389-2406, 2018, doi: 10.1109/COMST.2018.2812301.

[12] S. Chen *et al.*, "Internet of Things Based Smart Grids Supported by Intelligent Edge Computing," *IEEE Access*, vol. 7, pp. 74089-74102, 2019, doi: 10.1109/ACCESS.2019.2920488.

[13] S. P. Öztürk, "The era of digital transformation: Visualizing the geography of e-commerce usage in Turkey," *Environment and Planning A: Economy and Space*, vol. 53, no. 6, pp. 1241-1243, 2021, doi: 10.1177/0308518X211007798.

[14] W. Reinartz, N. Wiegand, and M. Imschloss, "The impact of digital transformation on the retailing value chain," *International Journal of Research in Marketing*, vol. 36, no. 3, pp. 350-366, 2019, doi: 10.1016/j.ijresmar.2018.12.002.

[15] F. Bellalouna, "Industrial Case Studies for Digital Transformation of Engineering Processes using the Virtual Reality Technology," *Procedia CIRP*, vol. 90, pp. 636-641, 2020, doi: 10.1016/j.procir.2020.01.082.
[16] S. E. Zaharia and C. V. Pietreanu, "Challenges in airport digital transformation," *Transportation Research Procedia*, vol. 35, pp. 90-99, 2018, doi: 10.1016/j.trpro.2018.12.016.
[17] S. Albukhitan, "Developing Digital Transformation Strategy for Manufacturing," *Procedia Computer Science*, vol. 170, pp. 664-671, 2020, doi: 10.1016/j.procs.2020.03.173.
[18] A. I. Urintsov, O. V. Staroverova, N. A. Mamedova, M. A. Afanasev, and M. S. Klyachin, "Consulting of Choice of Information System in the Conditions of Digital Transformation of Business," in *2019 International Conference* "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), 23-27 Sept. 2019, pp. 167-169, 2019, doi: 10.1109/ITQMIS.2019.8928307.
[19] R. Neugebauer, "Digital Information-The “Genetic Code” of Modern Technology," in *Digital Transformation*, R. Neugebauer Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 1-7.
[20] D. W. Fellner, "Virtual Reality in Media and Technology," in *Digital Transformation*, R. Neugebauer Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 19-41.
[21] K. Müller, H. Schwarz, P. Eisert, and T. Wiegand, "Video Data Processing," in *Digital Transformation*, R. Neugebauer Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 43-62.
[22] K. Brandenburg and C. Sladeczek, "Audio Codecs," in *Digital Transformation*, R. Neugebauer Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 63-77.
[23] G. Brzuchalski and G. Pastuszak, "Hardware implementation of the transformation module of the MPEG-4 AAC standard," *IFAC Proceedings Volumes*, vol. 43, no. 24, 2010, pp. 205-208, doi: 10.3182/20101006-2-PL-4019.00039.
[24] A. A. Pflaum and P. Gölzer, "The IoT and Digital Transformation: Toward the Data-Driven Enterprise," *IEEE Pervasive Computing*, vol. 17, no. 1, pp. 87-91, 2018, doi: 10.1109/MPRV.2018.011591066.
[25] R. C. Basole, "Accelerating Digital Transformation: Visual Insights from the API Ecosystem," *IT Professional*, vol. 18, no. 6, pp. 20-25, 2016, doi: 10.1109/MITP.2016.105.
[26] M. Sajić, D. Bundalo, Z. Bundalo, and D. Pašalić, "Digital technologies in transformation of classical retail bank into digital bank," in *2017 25th Telecommunication Forum (TELFOR)*, 21-22 Nov. 2017, 2017, pp. 1-4, doi: 10.1109/TELFOR.2017.8249404.

BIOGRAPHIES OF AUTHORS

Abbas M. Al-Ghaili is a postdoctoral researcher at Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional (UNITEN), Malaysia since Feb, 2018 until present. He received his B.Eng. degree (with first class honors) in computer engineering from the University of Science and Technology, Sana'a, Yemen, in 2005 and the M. Sc. and Ph.D. degrees in computer systems engineering from Universiti Putra Malaysia (UPM), Serdang, Malaysia, in 2009 and 2013, respectively. His research interests include Internet of Things security, artificial intelligence, energy informatics, and advanced computer security. Dr. Al-Ghaili is a member of the International Association of Computer Science and Information Technology and the Universal Association of Computer and Electronics Engineers.

Hairoladenan Kasim received the bachelor’s degree in information technology from Universiti Utara Malaysia, in 1998, and the master’s degree and the Ph.D. degree in information management from Universiti Teknologi Mara, in 2007 and 2015, respectively. He is currently working with the Department of Informatics, College of Computing and Informatics, Universiti Tenaga Nasional. He has conducted research on information systems (business informatics); computing in social science, arts, and humanities; and computer and society. His most recent publication is Formulating a Digital Energy Hub Framework to Inculcate Knowledge Sharing Practices for Energy Sectors.

Naif Mohammed Al-Hada received the B.Sc. degree in physics from Thamar University, Yemen, in 2002, and the M.Sc. degree in applied radiation physics and the Ph.D. degree in nanoscience and nanotechnology from Universiti Putra Malaysia (UPM), in 2011 and 2015, respectively. He was a Postdoctoral Researcher with the Department of Physics, UPM, from 2015 to 2019. He was a Visiting Researcher with Universiti Teknologi Malaysia (UTM), Malaysia, from June 2019 to October 2019. He has been a Lecturer of physics with Dezhou University (DZU), China, since October 2019. His research interests include nanoparticles synthesis and applications, metallic oxides nanostructures and its antibacterial activity, binary oxide nanostructures for solar cells and sensor applications, renewable energy, polymer composites/nanocomposites, conducting polymer nanocomposites, semiconductor nanotechnology, and applied radiation.