IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Airline Management System

Madhuri Thorat Author[1], Srushti Bhonde Author[2], Harsh Patil Author[3], Srushti KaleAuthor[4],

Asst. Prof., Ms. P.L.Rahinj [Project Guide]

Department of Computer Engineering Author [5]

Department of Computer Engineering

RGOE College of Engineering , Karjule Harya , India

Abstract: With the development of science and technology, the structure of engineering system has become increasingly large and complex. In order to ensure the safety and stability of the system in operation, the reliability evaluation of complex system has become an important research field. However, previous studies on the reliability of multi-state systems did not take into account the multi-level performance sharing in the system, and it has been unable to accurately assess the reliability of such complex systems. Therefore, based on the actual engineering system, this paper proposes a multi-state system with multi-level performance sharing mechanism. On this basis, we established a system reliability evaluation model using universal generating function technique. Through numerical examples, the application of the model and analyze the influence of different parameters on system reliability are demonstrated. In addition, we also use genetic algorithm to optimize the allocation of components in the system, so as to improve the reliability of the system. Different from the previous studies on system reliability with common bus performance sharing, the system proposed in this study is more general.

Keywords: Online rental things, Access-based Consumption, Sharing economy, Collaborative consumption, Online renting platform

Index Terms: Common bus, performance sharing, multi-state system reliability, universal generating function (UGF), genetic algorithm (GA).

I. INTRODUCTION

At present, in this era of rapid development of science and technology, the modernization level of industrial production is gradually improving. Under this development trend, various engineering systems have gradually become huge and complex, showing the characteristics of multi-state and performance sharing, especially in power, communication, computer,intelligenttransportationandothersystemsabound with high techniques . As these systems play a vital role in the stable operation and development of society and economy, once the system fails, it may cause major economic lossesanddisastrousconsequencesthataffectsociety. Therefore, the research on the reliability of multi-state system

with performance sharing has received extensive attention from scholars. Multi-state system is a kind of complex system which can exhibit multiple performance states during operation. Murchland put forward the basic concept of reliability of multi-state system for the first time. Due to the use of the reliability theory of multi-state systems, complex systems of multiple states in practice can be modeled more accurately and many related reliability studies have been carried out for this area. For example, Eryilmaz three-state components, and used this model to evaluate the reliability of two wind power generation systems in different regions. Lisnianski *et al*,proposed a multi-state Markov evaluation model based on historical data generating unit in the power system. Mo *et al*. proposed a reliability evaluation method for multi-state series-parallel systems based on multi-value decision diagrams. further discussed the reliability of a multi-state system with performance sharing, which is composed of multiple k-out-n subsystems. studied the instantaneous availability of a repairable system. For example, Jia *et al*. propose dareliabilitye valuation method formulti-state power system with performance sharing mechanism to alleviate the imbalance between supply and demand in the actual power system. studied the stable availability of collaborative computing system and the optimal allocation of units in the system.

Generally, multi-level performance sharing mechanism exists in complex engineering systems to improve resource utilization and system reliability. Taking the power system as an example, if the power generation capacity of all power plants in a city of a province cannot meet its load demand, other cities in this province can provide it with the necessary power through municipal transmission lines. When the power generation of the entire province is not enough to cover its load, other provinces in the same region can provide electricity for it through provincial transmission lines. When the power generation capacity of the entire region is deficient, it can borrow electricity from other regions, thus forming a multi-level power sharing power system. This mechanism for sharing performance through multi-level common bus is called multi-level performance sharing mechanism.

As the scale of the engineering system gradually expands, its structure becomes more and more complex, and system failures caused by design errors and unit failures are not uncommon. Therefore, in order to avoid serious consequences, it is usually necessary to carry out reliability evaluations for such large and complex systems. However, up to now, there is no literature considering the reliability of multi-state system with multi-level common bus performance sharing. In addition, in practical engineering systems, transmission loss is one of the important characteristics of the performance sharing mechanism. If the performance loss during the transmission process is ignored, the system reliability will be overestimated. The existing multi state system reliability evaluation model can no longer accurately describe the state of this complex system and evaluate its reliability.

Gsystemwithcommonbusperformancesharing.Su*etal*. further discussed the reliability of a multi-state system with performance sharing, which is composed of multiple k-out-n subsystems. studied the instantaneous availability of a repairable system. For example, Jia *et al*. propose dareliabilitye valuation method formulti-state power system with performance sharing mechanism to alleviate the imbalance between supply and demand in the actual power system. studied the stable availability of collaborative computing system and the optimal allocation of units in the system.

Generally, multi-level performance sharing mechanism exists in complex engineering systems to improve resource utilization and system reliability. Taking the power system as an example, if the power generation capacity of all power plants in a city of a province cannot meet its load demand, other cities in this province can provide it with the necessary power through municipal transmission lines. When the power generation of the entire province is not enough to cover its load, other provinces in the same region can provide electricity for it through provincial transmission lines. When the power generation capacity of the entire region is deficient, it can borrow electricity from other regions, thus forming a multi-level power sharing power system. This mechanism for sharing performance through multi-level common bus is called multi-level performance sharing mechanism.

As the scale of the engineering system gradually expands, its structure becomes more and more complex, and system failures caused by design errors and unit failures are not uncommon. Therefore, in order to avoid serious consequences, it is usually necessary to carry out reliability evaluations for such large and complex systems. However, up to now, there is no literature considering the reliability of multi-state system with multi-level common bus performance sharing. In addition, in practical engineering systems, transmission loss is one of the important characteristics of the performance sharing mechanism. If the performance loss during the transmission process is ignored, the system reliability will be overestimated. The existing multi state system reliability evaluation model can no longer accurately describe the state of this complex system and evaluate its reliability.

Therefore, this paper proposes a reliability evaluation model for multi-state system that comprehensively considers multi-level performance sharing and transmission loss

The model is constructed based on the universal generating function (UGF) technique, which is widely used to establish the reliability evaluation model of the multi-state system since it is flexible and effective in studying systems with multiple states and complex structures. Moreover, when the system structure and parameters are determined, different component allocation schemes will also have an effect on system reliability. In this paper, genetic algorithm (GA) is used to optimize the allocation of components in the system, so as to optimize the system reliability. Compared with previous studies, the model and method

constructed in this paper are more general, and they are suitable for reliability evaluation and optimization of multi-state systems with any layer.

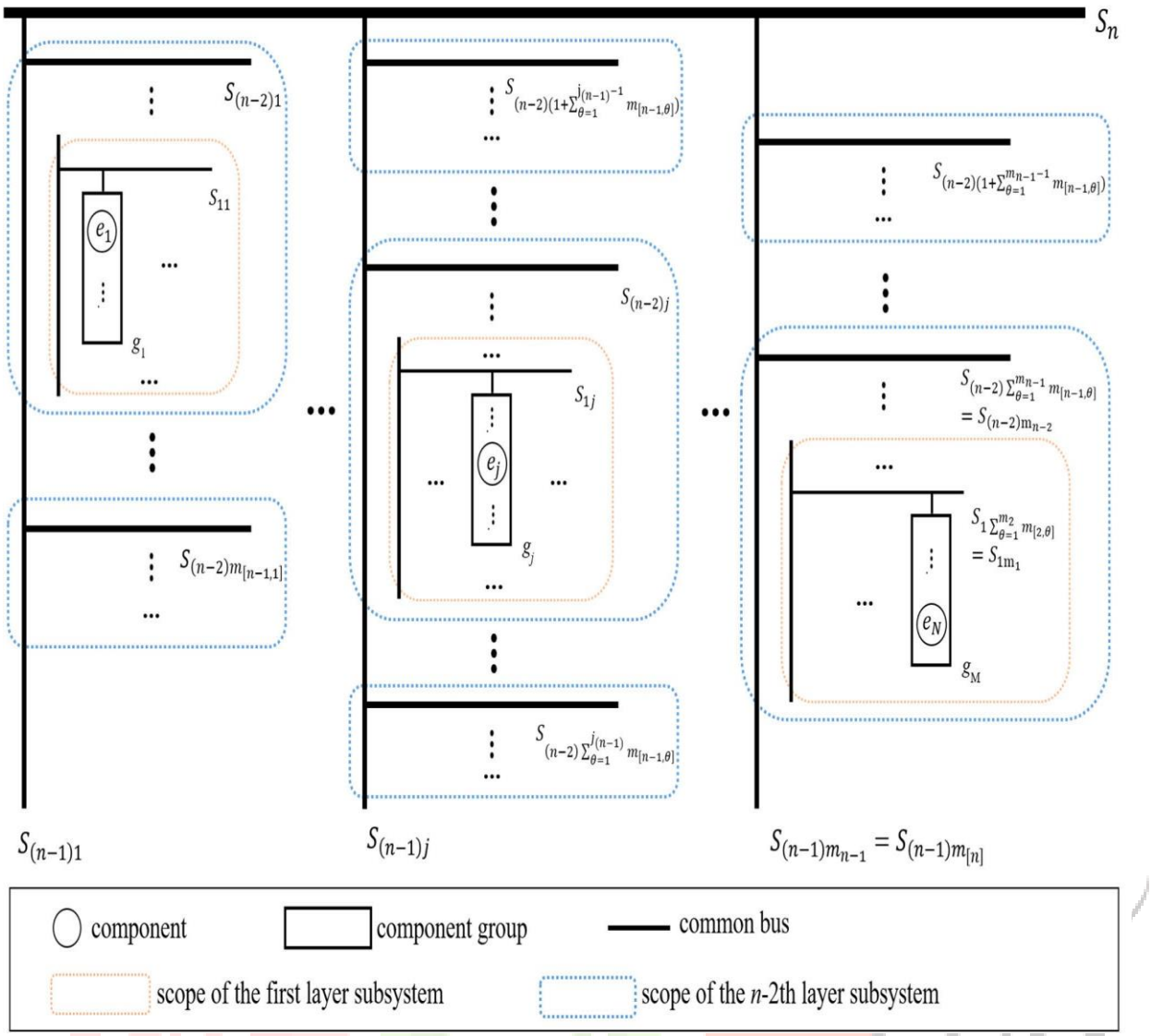
Theremainingofthispaperisarrangedasfollows.Thesecond section describes the structure of a multi-state system with multi-level common bus performance sharing. The third section proposes a system reliability evaluation algorithm based on the UGF technique. The fourth section introduces the component allocation mechanism, and the algorithm to optimize the component allocation. The fifth section gives some examples to illustrate the application of the proposed model, and analyzes the effect of different parameters on the system reliability. Finally, the full text is summarized in the sixth section.

II. NOTATIONS AND SYSTEM DESCRIPTION

In this paper, we assume that a complex system is composed of *n*-layer subsystems. The system structure is shown in Figure1. There is a common bus in each layer subsystem to promote performance sharing. For ease of understanding, we regard this complex system as an *n*th layer subsystem, which is composed of $m_{[n]}$ subsystems of *n*-1th layer, connected to an *n*th level common bus. Among them, the *j*th subsystem of *n*-1th layer is composed of $m_{[n-1,j]}$ subsystems of *n*-2th layer, which are connected to an *n*-1th level common bus. By analogy, the *j*th subsystem of first layer is composed of $m_{[1,j]}$ component groups, which are connected to a first level common bus. Finally, the component group g_j is composed of $m_{[g,j]}$ components in parallel, and each component group has

random performance requirements $W_{[g,j]}$ that need to be met. As the basic unit of the system, component e_j can generate random performance $X_{[e,j]}$. In addition, the components are independent of each other, component is not affected by the

Since this system has the multi-level performance sharing mechanism, if the performance of the component group can meet its own performance requirements, the surplus performance can be shared with other component groups connected to the same common bus, so that this subsystem can continue to share performance with other subsystems connected on the same common bus until passing the last level of common bus. However, sharing performance on the common bus is not completely free, so we assume that the common bus in each layer of subsystems has transmission capacity limitations, and the transmission capacity limitations are different. If the total amount of performance shared by the subsystem through the corresponding level common bus exceeds the transmission capacity limit of the common bus, the subsystem fails. In addition, if the *i*-1th layer subsystems in a certain *i*th layer subsystem share the performance with each other, the shared performance will occupy not only the transmission capacity of the *i*th level common bus, but also the transmission capacity of their internal *i*-1th level to first level



III. SYSTEM RELIABILITY EVALUATION MODEL

The UGF technique is a method of representing the probability distribution of multi-state system performance, which is widely used in the research of reliability analysis and optimization of multi-state system.

The UGF is a polynomial used to represent the distribution of a discrete random variable. The exponent represents all possible realization values of the random variable, and the coefficient is the probability corresponding to the realized value. This algorithm is used as a basic tool for the probability calculation of discrete random variables, and its expression is polynomial summation.

Suppose all possible values of discrete random variable X are $x(b)$, b = 1,2,...,B, and the probability of occurrence corresponding to all values is $P\{X = x(b)\} = p(b)$, b = 1,2,...,B, the UGF of the discrete random variable X is:

$$B\ u(z) = {}^{X}p(b) \cdot z^{x(b)}.\ b=1$$

In this paper, we use the UGF technique to establish the following system reliability evaluation model.

Based on the above definition, assuming that the performance of the component $X_{[e,j]}$ also presents a discrete random distribution. Then the probability distribution of the performance of the component e_j can be expressed as the following UGF_e:

$$u^{[e,j]}(z) = \sum_{b[e,j]=1}^{B[e,j]} p_{[e,j]}\left(b_{[e,j]}\right) \cdot zx[e,j](b[e,j]),$$

In the Eq. (1), $x_{[e,j]}\left(b_{[e,j]}\right)$ represents the possible performance value of the component e_j, and $p^{[e,j]}\left(b_{[e,j]}\right)$ represents the probability that the performance value of the component is $x^{[e,j]}\left(b_{[e,j]}\right)$. There are $B_{[e,j]}$ possibilities.

Because the component group g_j is composed of components in the set $M_{[g,j]}$, the performance of the component group g_j is equal to the sum of the cumulative performance of the $m_{[g,j]}$ componentsthatmakeupthecomponentgroup.Among them, the cardinality of the set $M_{[g,j]}$ is equal to the number of components in the set, that is, $|M_{[g,j]}| = m_{[g,j]}$.

Therefore, the probability distribution of the performance of the component group g_j can be expressed as the following UGF_g:

$$\alpha_{[g,j]}(z) = \oplus\left\{u_{[e,\varepsilon]}(z),\ldots,u^{[e,\tau]}(z)\right\}$$

$$= \begin{cases} \sum_{b_{[e,\varepsilon]}=1}^{B_{[e,\varepsilon]}} p_{[e,\varepsilon]}\left(b_{[e,\varepsilon]}\right) \cdot z^{x_{[e,\varepsilon]}\left(b_{[e,\varepsilon]}\right)}, \ldots, \sum_{b_{[e,\tau]}=1}^{B_{[e,\tau]}} p_{[e,\tau]}\left(b_{[e,\tau]}\right) \cdot z^{x_{[e,\tau]}\left(b_{[e,\tau]}\right)} \\ \end{cases}$$

$$B[e,\varepsilon]B^{[e,\tau]}\left(\prod_{k\in M_{[g,j]}} p_{[e,k]}\left(b_{[e,k]}\right)\right)$$

$$= X \ldots X \prod_{k\in M_{[g,j]}} x_{[e,k]}(b_{[e,k]})\ b_{[e,\varepsilon]}=1\ b_{[e,\tau]}=1 \cdot z$$

$$\beta_{[g,j]}(z) = \sum_{b[g,j]=1}^{B[g,j]} p_{[g,j]}\left(b_{[g,j]}\right) \cdot z^{x_{[g,j]}\left(b_{[g,j]}\right)},$$

where $j \in \{1,2,\ldots,N\}$. $\sum_{\theta=0}^{j} m_{[g,\theta]},\ m_{[g,0]} = 0.$

Since each component group g_j has requirements that need to be met, and the performance requirements $W_{[g,j]}$ obey a discrete random distribution,the probability distribution ofits performance requirements can be expressed as the following UGF_w:

$$\beta_{[g,j]}(z) = \sum_{b'_{[g,j]}=1}^{B^0_{[g,j]}} p'_{[g,j]}\left(b'_{[g,j]}\right) \cdot z^{w_{[g,j]}\left(b'_{[g,j]}\right)},$$

where $j \in \{1,2,\ldots,M\}$.

In the Eq. (3), $w_{[g,j]}\left(b'_{[g,j]}\right)$represents the possible requirements value of the component group g_j, there are $B^0_{[g,j]}$ types in total, and $p'_{[g,j]}\left(b'_{[g,j]}\right)$ represents its corresponding probability.

From this, we can get the UGF_g' of the component group in all states.

$$\gamma_{[g,j]}(z) = \otimes\left\{\alpha_{[g,j]}(z), \beta_{[g,j]}(z)\right\}$$

B

$b[\sum^{[g,j]} p_{[g,j]}(b_{[g,j]}) \cdot z^{x_{[g,j]}(b_{[g,j]})} g,j]=1$,

$= \otimes \cdot z^{w_{[g,j]}(b'_{[g,j]})}$ $B0[g,j]$

$b0[gP,j]=1\ p^{'}_{[g,j]}(b'_{[g,j]})$

$\sum^{B'_{[g,j]}} (p_{[g,j]}(b_{[g,j]}) \quad _{[g,j]}(b_{[g,j]}))$

$B[g,j]\times \ _p0$ (0 X

$= \quad _{[g,j]=1}\ b'_{[g,j]=1} \cdot z^{\{x_{[g,j]}(b_{[g,j]}),w_{[g,j]}(b'_{[g,j]})\}}$

b

$B00$

$= \sum^{[g,j]} p''_{[g,j]}(b''_{[g,j]}) \cdot z^{\{x_{[g,j]}(b''_{[g,j]}),w_{[g,j]}(b''_{[g,j]})\}}$,

$b''_{[g,j]=1}$

where $j \in \{1,2,...,M\}$, $B^{00}_{[g,j]}$ indicates that the number of performance values and requirements values that can be achieved simultaneously by the component group g_j, and $p''_{[g,j]}(b''_{[g,j]})$ is the corresponding probability.

If the component group g_j fails to meet the requirements, the component group needs to borrow performance from other component groups with surplus performance through the common bus to meet their requirements. The borrowed performance is $w_{[g,j]}(b''_{[g,j]}) - x_{[g,j]}(b''_{[g,j]})$. If the component group meets the requirements, the component group can lend performance to other component groups with deficient performance through the common bus to save resources. The lent performance is $x_{[g,j]}(b''_{[g,j]}) - w_{[g,j]}(b''_{[g,j]})$.

Then the probability distribution of the deficient or surplus performance of the component group g_j can be expressed as the following UGF$_g$'': $u = \varphi(\gamma_{[g,j]}(z))$

$= \sum^{g,j} \max\{w_{[g,j]}(b''_{[g,j]}) - x_{[g,j]}(b''_{[g,j]}), 0\}$ $B[00]$ $p''_{[g,j]}(b''_{[g,j]})$

, (5)

$w_{[g,j]}(b''_{[g,j]}), 0\}$ $\max\{x_{[g,j]}(b''_{[g,j]}) -$

$b00$

$\cdot z$

where $j \in \{1,2,...,M\}$.

In the Eq. (5), $\max\{w_{[g,j]}(b''_{[g,j]}) - x_{[g,j]}(b''_{[g,j]}), 0\}$ represents the deficient performance value of the component group g_j, and $\max\{x_{[g,j]}(b''_{[g,j]}) - w_{[g,j]}(b''_{[g,j]}), 0\}$ represents the surplus performance value of the component group g_j. In addition, in any state, the performance of the component group g_j can only be expressed in one of the following three situations: (1)The performance just meets the requirements; (2)The performance is deficient; (3)The performance is surplus. That is

$\{\max\{w_{[g,j]}(b''_{[g,j]}) - x_{[g,j]}(b''_{[g,j]}), 0\}$

$_{[g,j]}(b''_{[g,j]}), 0\}$ $_{[g,j]}(b''_{[g,j]}) -$

, min $_n$= 0.

max *xw*

Because the first layer subsystem S_{1j} is composed of component groups in the set $M_{[1,j]}$, the performance of the first layer subsystem S_{1j} is equal to the sum of the cumulative performance of the $m_{[1,j]}$ component groups that make up the subsystem. In the same way, the deficient and surplus performance of the first layer subsystem S_{1j} is also equal to the cumulative sum of the deficient and surplus performance of the $m_{[1,j]}$ component groups that make up the subsystem. Among them, the cardinality of the set $M_{[1,j]}$ is equal to the number of components in the set, that is, $|M_{[1,j]}| = m_{[1,j]}$.

Therefore, the probability distribution of the deficient and surplus performance of the first layer subsystem S_{1j} can be expressed as the following UGF_{S1}:

$$u_{[1,j]}(z) = \oplus\{u_{[g,\varepsilon]}(z),\ldots,u_{[g,\tau]}(z)\} = \sum_{b_{[1,j]}=1}^{B[1,j]} p_{[1,j]}(b_{[1,j]}) \cdot z^{\{d_{[1,j]}(b_{[1,j]}),s_{[1,j]}(b_{[1,j]})\}}, \quad (6)$$

where $j \in \{1,2,\ldots,m^1\}$, $\varepsilon = 1 + \sum_{\theta=0}^{j-1} m_{[1,\theta]}$, $\tau = \sum_{\vartheta=0}^{j} m_{[1,\vartheta]}$, $m_{[1,0]} = 0$.

In Eq. (6), $u_{[g,\varepsilon]}(z),\ldots,u_{[g,\tau]}(z)$ represents the UGF_g'' of the probability distribution of the deficient and surplus performance of all component groups in the first layer subsystem S_{1j}. Because the deficient and surplus performance of the first layer subsystem is equal to the cumulative sum of the deficient and surplus performance of the component groups that make up the subsystem. Therefore, in the second equation of Eq. (6), $d_{[1,j]}(b_{[1,j]})$ represents the overall deficient performance of the first layer subsystem S_{1j}, and $s_{[1,j]}(b_{[1,j]})$ represents the overall surplus performance of the first layer subsystem S_{1j}. In addition, $p_{[1,j]}(b_{[1,j]})$represents the probability when its deficient and surplus performance are $d_{[1,j]}(b_{[1,j]})$ and $s_{[1,j]}(b_{[1,j]})$ respectively, where

$\sum_{b=1}^{B_{[1,j]}} p_{[1,j]}(b_{[1,j]}) = 1$, and any first layer subsystem S_{1j} has $B_{[1,j]}$ possible deficient and surplus performance values.

Because all component groups in the first layer subsystem S_{1j} are connected to a first level common bus, these component groups can share performance through this common bus, but the total amount of shared performance must not exceed the limit of the common bus transmission capacity $C_{[1,j]}$. If the limit is exceeded, the system will fail. Therefore, if the deficient performance of the first layer subsystem S_{1j} is greater than the transmission capacity of the first level common bus, that is, $d_{[1,j]}(b_{[1,j]}) - C_{[1,j]} > 0$. It means that the subsystem cannot make up for the deficient performance after sharing the performance, and cannot meet the requirements of the component groups in this subsystem, resulting in system failure. When calculating the system reliability, the probability of this state can be ignored. If the deficient performance of the first layer subsystem S_{1j} is less than or equal to the transmission capacity of the first level common bus, that is, $C_{[1,j]} - d_{[1,j]}(b_{[1,j]}) \geq 0$. It shows that the subsystem can make up for deficient performance through performance sharing. At this time, the system may have two states. One state is $d_{[1,j]}(b_{[1,j]}) > s_{[1,j]}(b_{[1,j]})$, which means that the performance provided by the component group with surplus performance in the first layer subsystem cannot make up for the component group with deficient performance. The subsystem still needs to borrow performance from other subsystems at the same layer, and the total amount of borrowed performance is $d_{[1,j]}(b_{[1,j]}) - s_{[1,j]}(b_{[1,j]})$. The other state is $s_{[1,j]}(b_{[1,j]}) \geq d_{[1,j]}(b_{[1,j]})$, which means that the component groups with surplus performance in the first layer

subsystem can provides enough performance to make up for the component group with deficient performance. After sharing, the remaining performance can be lent to other

$$U_{[1,j]}(z) = f\,u^{[1,j]}(z))$$

subsystems at the same level, but the total amount of sharing shall not exceed the limit of the transmission capacity of the common bus, the total amount of lent performance is

$$\min\left\{s_{[1,j]}\left(b_{[1,j]}\right) - d_{[1,j]}\left(b_{[1,j]}\right),\ C_{[1,j]} - d_{[1,j]}\left(b_{[1,j]}\right)\right\}.$$

Then the probability distribution of the performance that the first layer subsystem S_{1j} still needs to borrow or can lend at most can be expressed as (7), shown at the bottom of the page, UGF_{S1}', where $j \in \{1,2,...,m_1\}$. $I()$ is a conditional function. When the condition in brackets is satisfied, the result is 1, otherwise it is 0.

If there is performance loss in the transmission process, and the total amount of performance loss is approximately proportional to the total amount of performance transmission. Then the probability distribution of the performance that the first layer subsystem S_{1j} still needs to borrow or can lend at most can be expressed as (8), shown at the bottom of the page, UGF_{S1}'', where ω represents the loss rate of performance during transmission.

Because the performance is lost during the transmission process, the system can work normally if and only if the total amount of performance transmitted over the common bus is less than or equal to the transmission capacity limit. Therefore, under the condition of $d_{[1,j]}\left(b_{[1,j]}\right)/(1-\omega) \le C_{[1,j]}$, if $d_{[1,j]}\left(b_{[1,j]}\right) > (1-\omega)\,s_{[1,j]}\left(b_{[1,j]}\right)$, it means that the total amount of effective transmission of surplus performance in the subsystem cannot meet its deficient performance. The subsystem still needs to borrow performance, and the total amount is $d_{[1,j]}\left(b_{[1,j]}\right) - (1-\omega)\,s_{[1,j]}\left(b_{[1,j]}\right)$.

If $(1-\omega)s_{[1,j]}\left(b_{[1,j]}\right) \ge d_{[1,j]}\left(b_{[1,j]}\right)$, it means that the total amount of effective transmission of surplus performance in the system can meet its deficient performance. After the shared performance of the system meets its deficient performance, the remaining performance can still be lent, but it cannot exceed the transmission capacity limit of its common bus, that is, the total amount of remaining performance is

$$\min\left\{\begin{matrix} s_{[1,j]}\left(b_{[1,j]}\right) - d_{[1,j]}\left(b_{[1,j]}\right)/(1-\omega), \\ C_{[1,j]} - d_{[1,j]}\left(b_{[1,j]}\right)/(1-\omega) \end{matrix}\right\}.$$

Therefore, the probability distribution of the deficient and surplus performance of the nth layer subsystem S_n can be expressed as the following UGF_{Sn}:

$$u^{[n]}(z) = \oplus\left\{U_{[n-1,1]}(z),...,U^{[n-1,m_{[n]}]}(z)\right\}$$

$$U_{[i,j]}(z) = f\,u^{[i,j]}(z))$$

$$\text{X} \quad {}_{[n]}\left(b_{[n]}\right)\cdot z^{\{d_{[n]}(b_{[n]}),s_{[n]}(b_{[n]})\}} \quad {}^{B[n]}_{b[n]=1} = p,$$

where $m_{[n]}$ represents the number of n-1th layer subsystems in the nth layer subsystem.

In the second equation of Eq. (12), $d_{[n]}(b_{[n]})$ represents the total amount of deficient performance of the whole system, and $s_{[n]}(b_{[n]})$ represents the total amount of surplus performance of the whole system. Therefore, the system can work normally if and only when the total amount of deficient performance of the system is less than or equal to the total amount of surplus performance of the system and the transmission capacity of the nth level common bus.

Therefore, the overall reliability of the system can be calculated by the following equation:

$$R = \sum_{b_{[n]}=1}^{B[n]} I\left(x_{[n]}(b_{[n]}) \le \min\left\{s_{[n]}(b_{[n]}), C_{[n]}\right\}\right) P_{[n]}(b_{[n]})$$

If there is performance loss in transmission, the system can only work normally if the system just meets the deficient performance by adopting the performance sharing mechanism, and the total amount of transmission through the common bus should be less than or equal to the total amount of surplus performance and the transmission capacity of the common bus. Therefore, the overall reliability of the system is

$$= \sum_{b}^{B} I\left(\frac{[n]([n]}{-} \le \min\left\{s_{[n]}(b_{[n]}), C_{[n]}\right\}\right)^{[n]} \quad d \quad (b \quad) \quad ! \qquad (1 \quad \omega) \quad R \qquad P_{[n]}(b$$

IV. OPTIMIZE COMPONENT ALLOCATION

In this section, we establish the component allocation mechanism, and define the position of each component in the system. In addition, we use GA to optimize the allocation of components in the system, which is of practical significance to improve the reliability of the system.

m_1 first layer subsystems, m_2 second layer subsystems...and so on, and finally form m_n nth layer subsystems. In the initial construction of the system, the whole system is regarded as an nth layer subsystem, so m_n is essentially equal to 1, that is $m_n \equiv 1$.

According to the previous definition, during the operation of the system, each component group g_j has a requirements $W_{[g,j]}$ that needs to be met. In addition to using the common bus sharing performance to improve system reliability, the initial component allocation can also be used to meet the requirements of each component group as much as possible to reduce the probability of system failure. In practical engineering design, optimizing component allocation plays an extremely important role in improving system reliability. Therefore, it is necessary to plan the component allocation before the system runs.

In this study, we assume that the system structure is known and fixed, that is, the number of subsystems and component groups at different layers in the system, and the relationship between them are determined. Through the following operations, the subsystems of different layers that each component group belongs to can be identified quickly.

the set E_r should be allocated to the $r - m_{[1,0]} + \cdots + m_{[1,j]}$th component groups of the j+1th subsystem of first layer.

In this case, let $j + 1 = r_1$, when r_1 satisfies the

following conditions, $m[2,0] + \cdots + m[2,j] < r1 \le m[2,0] + \cdots + m[2,j+1], m[2,0]$

$= 0,$

the set E_r should be allocated to the $r - m_{[1,0]} + \cdots + m_{[1,j]}$th component groups of the $r_1 - m_{[2,0]} + \cdots + m_{[2,j]}$th subsystem of first layer of the j+1th subsystem of second layer.

(3)By analogy,let$j$+1 = r_i,whenr_i satisfiesthe following conditions,

$m[i+1,0]^{+\cdots+}m[i+1,j] < ri \le m[i+1,0]^{+\cdots+}m[i+1,j+1],$
$m[i+1,0] = 0,$

the set E_r should be allocated to the $r - m[1,_0] + \cdots + m[1,_j]$th component groups of ...of the $ri - (m_{+} + \cdots + m_{+})$[$i$ 1,0] [i 1,j] th subsystem of ith layer of the j+1th subsystem of i+1th layer.

(4) Until $i = n - 2$, let $j + 1 = r_n - 2$, when $r_n - 2$ satisfies the following conditions,

$m[n-1,0]^{+\cdots+}m[n-1,j] < rn-2 \le m[n-1,0]^{+\cdots+}m[n-1,j+1],$
$m[n-1,0] = 0,$

the set E_r should be allocated to the $r - m[1,_0] + \cdots + m[1,_j]$th component groups of ...of the $r_{n-2} - (m_{[n-1,0]} + \cdots + m_{[n-1,j]})$th subsystem of n-2th layer of the j+1th subsystem of n-1th layer.

At this time, the set E composed of N components is divided into M disjoint sets $E_r, r \in \{1,...,M\}$. In the allocation process, each component e_j has M different options, and there are M^N allocation schemes in total.

Suppose the allocation scheme is $L^{(a)}, a \in \{1,...,M^N$, and the system reliability is different under different allocation schemes. Therefore, the optimal component allocation scheme is the scheme that maximizes the system reliability, which is

$\max R(L(a)), a \in n1,...,M^N$.

Accordingtothedefinitioninthispaper,thesystemreliability of different schemes can be obtained by However, for a complex system with numerous components, it is not easy to find the optimal component allocation scheme. Because the number of component allocation schemes is M^N and exhibits an exponential growth. It is necessary to calculate M^N times to find the scheme that maximizes the system reliability. Therefore, in order to simplify the calculation process, we use GA to solve the component allocation problem.

V. GENETIC ALGORITHM

In previous studies, GA has been proven to be an effective optimization method to solve a large number of complex problems in engineering systems . Based on Darwin's theory of evolution, the algorithm simulates the process of biological evolution to search for the optimal solution globally. The GA starts with the initial population that represents part of the feasible solution to the optimization problem. According to the individual's adaptation to the environment, select some individuals with higher fitness to reproduce and produce the next generation (the new solution). Gene crossover and mutation occur during reproduction. Crossover is to use the chromosomes of a pair of preferred

individuals as parent genes, and form a new offspring gene after cross recombination. The offspring formed by the crossover will inherit some of the traits of their parents. Mutation is to make minor mutation in the offspring gene, so as to avoid the optimization results converging to the local optimum. After n generations of natural selection, the offspring with low fitness will be gradually eliminated, and finally the optimal solution with the highest fitness will be searched for.

VI. ENCODING AND DECODING OF THE SOLUTION

When using GA to solve specific problems, the coding process, decoding process, calculation process and fitness value of the solution must be defined.

The first step in writing a GA is coding. Therefore, we assume that any allocation scheme can be encoded as a string $H = \{h_1, h_2, \ldots, h_N\}$, where $h_i = 1, 2, \ldots, M$ represents the allocation scheme of component e_i, that is, which component group the component e_i is allocated to. Conversely, the allocation of any component can also be decoded from the string.

The crossover and mutation operations of strings in GA are defined as follows. Randomly select a pair of parental strings H_1 and H_2 from the population for genetic crossover, then any character h_i in the offspring string O has a 50% probability of coming from the parental string H_1 or H_2. In the process of mutation, the character h_i at the random position of the offspring string O may change slightly.

In addition, the new solutions generated after crossover and mutation need to be decoded and evaluated for fitness. In this optimization problem, the fitness function for evaluating individual fitness is the system reliability R in section III.

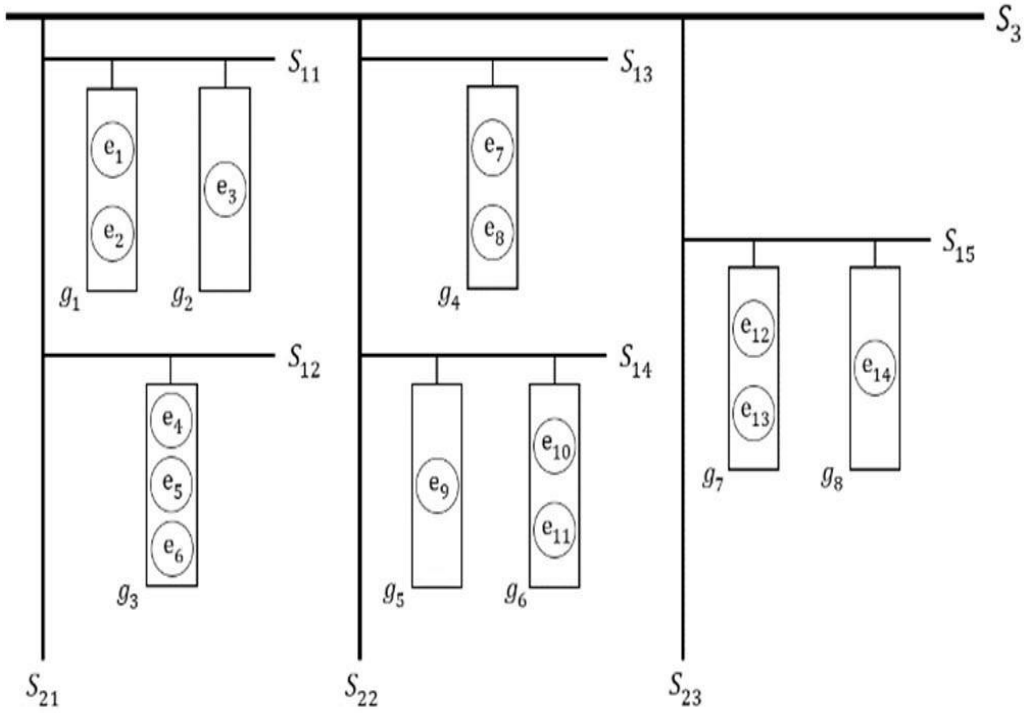
VII. NUMERICAL EXAMPLES

In this section, first of all, we use a set of numerical values to demonstrate the system reliability evaluation model established in section III. Secondly, we analyze the effect of different parameters in the system on the reliability. Finally, we use the computer programming language Python to write GA to solve the optimal component allocation scheme of the system, so as to study how to allocate the components to improve the system reliability.

We assume that the system structure is shown in Figure 2. The system is a three-layer multi-state system with 14 components, which are allocated to 8 different component groups, namely $E_1 = \{e_1, e_2\}$, $E_2 = \{e_3\}$, $E_3 = \{e_4, e_5, e_6\}$, $E4 = \{e7, e8\}$, $E5 = \{e9\}$, $E6 = \{e10, e11\}$, $E7 = \{e12, e13\}$, $E8 = \{e14\}$.

The probability distribution of the performance of the 14 components in the system is shown in Table 1.

The probability distribution of the performance requirements of the 8 component groups in the system is shown in Table 2.



The system shown above has three-level common bus sharing performance, a total of six. Its transmission capacity limit is $C[1,1] = C[1,2] = C[1,3] = C[1,4] = C[1,5] = 5$, $C_{[2,1]} = C_{[2,2]} = C_{[2,3]} = 10, C_{[3]} = 15$respectively.Ifthere is performance loss during transmission, assume that the line loss rate $\omega = 0.1$.

Use the system reliability evaluation model to calculate the system reliability:

(1) Probability distribution of component performance

$u_{[e,1]}(z) = 0.1z^0 + 0.9z^5$ $u_{[e,2]}(z) = 0.2z^0 + 0.8z^{10}$ $u_{[e,3]}(z) = 0.15z^0 + 0.85z^{20}$ $u_{[e,4]}(z) = 0.1z^0 + 0.9z^{10}$ $u_{[e,5]}(z) = 0.4z^0 + 0.6z^{30}$ $u_{[e,6]}(z) = 0.25z^0 + 0.75z^{25}$ $u_{[e,7]}(z) = 0.3z^0 + 0.7z^{20}$ $u_{[e,8]}(z) = 0.05z^0 + 0.95z^{20}$ $u_{[e,9]}(z) = 0.2z^0 + 0.8z^{15}$ $u_{[e,10]}(z) = 0.5z^0 + 0.5z^{15}$ $u_{[e,11]}(z) = 0.25z^0 + 0.75z^{30}$ $u_{[e,12]}(z) = 0.1z^0 + 0.9z^{35}$ $u_{[e,13]}(z) = 0.15z^0 + 0.85z^{20}$ $u_{[e,14]}(z) = 0.4z^0 + 0.6z^{10}$

(2) The probability distribution of the performance of the component group

$\alpha_{[g,1]}(z) = 0.02z^0 + 0.08z^{10} + 0.18z^5 + 0.72z^{15}$ $\alpha_{[g,2]}(z) = 0.15z^0 + 0.85z^{20}$

$\alpha_{[g,3]}(z) = 0.01z^0 + 0.03z^{25} + 0.015z^{30} + 0.045z^{55} + 0.09z^{10} + 0.27z^{35} + 0.135z^{40} + 0.405z^{65}$ $\alpha_{[g,4]}(z) = 0.015z^0 + 0.32z^{20} + 0.665z^{40}$ $\alpha_{[g,5]}(z) = 0.2z^0 + 0.8z^{15}$ $\alpha_{[g,6]}(z) = 0.125z^0 + 0.375z^{30} + 0.125z^{15} + 0.375z^{45}$ $\alpha_{[g,7]}(z) = 0.015z^0 + 0.085z^{20} + 0.135z^{35} + 0.765z^{55}$ $\alpha_{[g,8]}(z) = 0.4z^0 + 0.6z^{10}$ $0.05z^{25} + 0.95z^{35}$ $\beta_{[g,4]}(z) = 0.2z^{10} + 0.8z^{30}$ $\beta_{[g,5]}(z) = 0.9z^5 + 0.1z^{20}$ $\beta_{[g,6]}(z) = 0.05z^{15} + 0.95z^{30}$ $\beta_{[g,7]}(z) = 0.4z^{20} + 0.6z^{40}$ $\beta_{[g,8]}(z) = 0.25z^5 + 0.75z^{10}$

(3) Probability distribution of deficient and surplus performance of component groups

$u[g,1](z)$

= 0.132z{10,0} + 0.014z{15,0} + 0.528z{0,0}

+0.11z{5,0} + 0.216z{0,5}

$u[g,2](z)$

= 0.0225z{5,0} + 0.1275z{15,0} + 0.1275z{0,15}

+0.7225z{0,5}

$u[g,3](z)$

= 0.086z{25,0} + 0.0095z{35,0} + 0.258z{0,0}

+0.0285z{10,0} + 0.129z{0,5} + 0.01425z{5,0}

(4) The probability distribution of the performance requirements of the component group

$\beta_{[}g,1](z) = 0.3z^{10} + 0.7z^{15}$ $\beta_{[}g,2](z) = 0.15z^{5} + 0.85z^{15}$ $\beta_{[}g,3](z)$ = +0.387z{0,30} + 0.04275z{0,20} + 0.0045z{15,0}

+0.0135z{0,10} + 0.00675z{0,15} + 0.02025z{0,40}

e_1		e_2		e_3		e_4		e_5		e_6		e_7	
P	x	p	x	p	x	p	x	p	x	p	x	p	x
0.10	0	0.20	0	0.15	0	0.10	0	0.40	0	0.25	0	0.30	0
0.90	5	0.80	10	0.85	20	0.90	10	0.60	30	0.75	25	0.70	20

e_8		e_9		e_{10}		e_{11}		e_{12}		e_{13}		e_{14}	
P	x	p	x	p	x	p	x	p	x	p	x	p	x
0.05	0	0.20	0	0.50	0	0.25	0	0.10	0	0.15	0	0.40	0
0.95	20	0.80	15	0.50	15	0.75	30	0.90	35	0.85	20	0.60	10

+0.387z{0,30} + 0.04275z{0,20} + 0.0045z{15,0}

+0.0135z{0,10} + 0.00675z{0,15} + 0.02025z{0,40}

$u[g,4](z)$

= 0.259z{10,0} + 0.012z{30,0} + 0.596z{0,10}

+0.133z{0,30} $u[g,5](z)$

= 0.26z{5,0} + 0.02z{20,0} + 0.72z{0,10}

$u[g,6](z)$

= 0.125z{15,0} + 0.11875z{30,0} + 0.375z{0,15}

+0.3625z{0,0} + 0.01875z{0,30}

$u[g,7](z)$

= 0.057z{20,0} + 0.009z{40,0} + 0.034z{0,0}

+0.513z{0,15} + 0.081z{5,0} + 0.306z{0,35}

$u[g,8](z)$

= 0.1z{5,0} + 0.3z{10,0} + 0.15z{0,5} + 0.45z{0,0}

(5) Probability distribution of deficient and surplus performance of the first layer subsystem

$u[1,1](z)$

= 0.07029z{15,0} + 0.01683z{25,0} + 0.01683z{10,15}

+0.09537z{10,5} + 0.01434z{20,0} + 0.001785z{30,0}

+0.001785z{15,15} + 0.037655z{15,5} + 0.01188z{5,0}

+0.06732z{0,15} + 0.38148z{0,5} + 0.002475z{10,0}

+0.014025z{5,15} + 0.084335z{5,5} + 0.02754z{0,20}

+0.15606z{0,10}

g_1		g_2		g_3		g_4	
p	w	p	w	p	w	p	w
0.30	10	0.15	5	0.05	25	0.2	10
0.70	15	0.85	15	0.95	35	0.8	30
g_5		g_6		g_7		g_8	
p	w	p	w	p	w	p	w
0.90	5	0.05	15	0.40	20	0.25	5
0.10	20	0.95	30	0.60	40	0.75	10

$u[1,2](z)$

= 0.086z{25,0} + 0.0095z{35,0} + 0.258z{0,0}

+0.0285z{10,0} + 0.129z{0,5} + 0.01425z{5,0}

+0.387z{0,30} + 0.04275z{0,20} + 0.0045z{15,0}

+0.0135z{0,10} + 0.00675z{0,15} + 0.02025z{0,40}

$u[1,3](z)$

= 0.259z{10,0} + 0.012z{30,0} + 0.596z{0,10}

+0.133z{0,30} $u[1,4](z)$

= 0.03975z{20,0} + 0.033375z{35,0} + 0.0975z{5,15}

+0.09425z{5,0} + 0.004875z{5,30} + 0.002375z{50,0}

+0.0075z{20,15} + 0.000375z{20,30} + 0.09z{15,10}

+0.0855z{30,10} + 0.27z{0,25} + 0.261z{0,10}

+0.0135z{0,40}

$u[1,5](z)$

= 0.0057z{25,0} + 0.0171z{30,0} + 0.00855z{20,5} +0.02565z{20,0} + 0.0009z{45,0} + 0.0027z{50,0}

+0.00135z\{40,5\} + 0.00405z\{40,0\} + 0.03985z\{5,0\}

+0.0183z\{10,0\} + 0.0051z\{0,5\} + 0.0153z\{0,0\}

+0.0513z\{5,15\} + 0.1539z\{10,15\} + 0.07695z\{0,20\}

+0.23085z\{0,15\} + 0.0243z\{15,0\} + 0.01215z\{5,5\}

+0.0306z\{5,35\} + 0.0918z\{10,35\} + 0.0459z\{0,40\}

+0.1377z\{0,35\}

1) THE PERFORMANCE OF THE COMPONENT

Taking the system established in section V-A as an example. We fix all parameters except the performance of the component, and increase the performance of all components in the system by 5 units in order to study the effect of different performance of components on system reliability. The calculation results are shown in Table 3 below.

The results show that under the condition that other parameters remain unchanged, regardless of whether there is performance loss during the transmission process, the system reliability will increase with the increase of the performance of the component. At the same time, we tested the two assumed transmission modes, that is, transmission without performance loss and transmission with performance loss. It has been proved that the system reliability will decrease with the loss of performance in the transmission process.

Reliability \ Transmission capacity	$\begin{bmatrix} C_{[1,j]}=0 \\ C_{[2,j]}=0 \\ C_{[3]}=0 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=5 \\ C_{[2,j]}=0 \\ C_{[3]}=0 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=5 \\ C_{[2,j]}=5 \\ C_{[3]}=0 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=5 \\ C_{[2,j]}=5 \\ C_{[3]}=5 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=10 \\ C_{[2,j]}=10 \\ C_{[3]}=5 \end{bmatrix}$
Without loss ($\omega=0$)	0.1101	0.1790	0.2103	0.2255	0.4766
With loss ($\omega=0.1$)	0.1101	0.1101	0.1101	0.1101	0.2104
Reliability \ Transmission capacity	$\begin{bmatrix} C_{[1,j]}=15 \\ C_{[2,j]}=15 \\ C_{[3]}=10 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=20 \\ C_{[2,j]}=15 \\ C_{[3]}=15 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=25 \\ C_{[2,j]}=25 \\ C_{[3]}=20 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=40 \\ C_{[2,j]}=35 \\ C_{[3]}=35 \end{bmatrix}$	$\begin{bmatrix} C_{[1,j]}=\infty \\ C_{[2,j]}=\infty \\ C_{[3]}=\infty \end{bmatrix}$
Without loss ($\omega=0$)	0.5921	0.6581	0.7518	0.8792	0.8907
With loss ($\omega=0.1$)	0.4786	0.5583	0.6803	0.8304	0.8579

2) THE PERFORMANCE REQUIREMENTS OF THE COMPONENT GROUP

Taking the system established in section V-A as an example.

We reassume C[1,1] = C[1,2] = C[1,3] = C[1,4] = C[1,5] = 25, $C_{[2,1]}$ = $C_{[2,2]}$ = $C_{[2,3]}$ = 20, $C_{[3]}$ = 15. In addition to the performance requirements, other parameters remain unchanged, so as to compare the system reliability under different performance requirements. The calculation results are shown in Table 4 below.

It can be seen from Table 4 that regardless of whether there is performance loss during the transmission process, when the performance requirements of the component group increase, the system reliability will decrease accordingly. This is the same as the definition of system reliability in this paper. Increasing the performance requirements of component groups will reduce the number of component groups that meet the requirements and reduce the overall reliability of the system.

3) THE TRANSMISSION CAPACITY OF THE COMMON BUS

Taking the system established in section V-A as an example. We fix all parameters except the transmission capacity of the common bus, and increase the transmission capacity of the common bus at all levels of the system in order to study the effect of different transmission capacities on system reliability. The calculation results are shown in Table 5 below.

From the calculation results, it can be seen that introducing the performance sharing mechanism into the system will improve the system reliability. Because, when the transmission capacity of the common bus increases, more units will meet the system requirements through sharing performance, thereby improving the overall reliability of the system. However, when the transmission capacity exceeds the total amount of performance that can be shared within the system, increasing the transmission capacity can no longer improve the system reliability. Secondly, under the different transmission capacity, the system reliability considering the performance loss is low. In addition, when the system has transmission loss and the transmission capacity is small, the reliability increase caused by the slight increase of transmission capacity is not obvious.

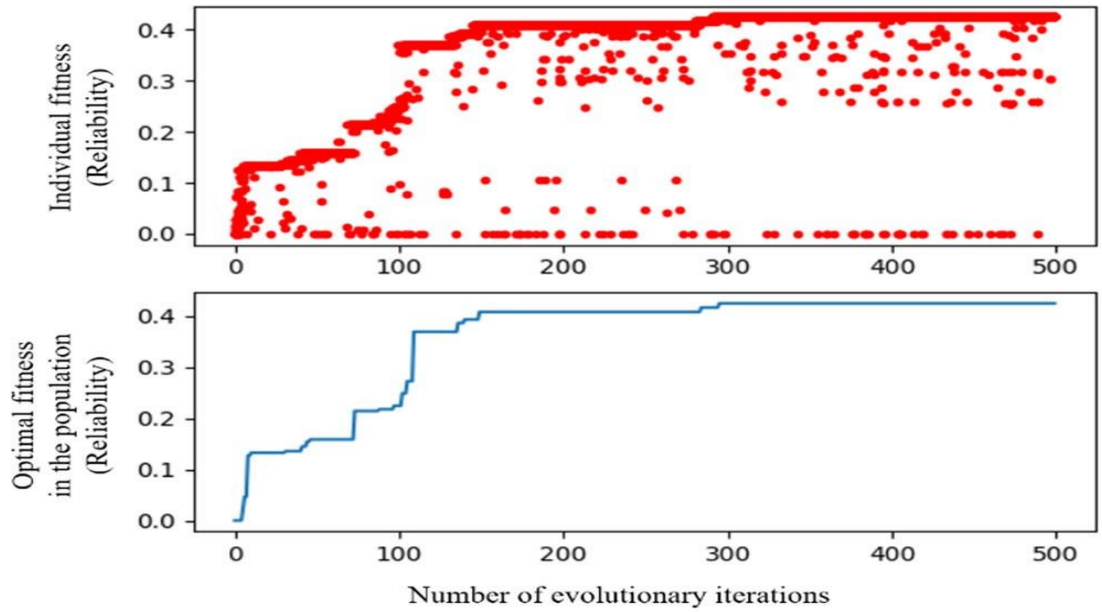
4) THE TRANSMISSION LOSS RATE

Taking the system established in section V-A as an example.

We reassume $C[1,1] = C[1,2] = C[1,3] = C[1,4] = C[1,5] = 25$, $C_{[2,1]} = C_{[2,2]} = C_{[2,3]} = 20$, $C_{[3]} = 15$. Other parameters except the transmission loss rate remain unchanged, so as to compare the system reliability under the different loss rates. The calculation results are shown in Table 6 below.

It can be seen from Table 6 that the system reliability will gradually decrease as the transmission loss rate increases. This shows that if there is performance loss in the transmission process, the higher the loss rate, the more performance loss, the fewer components can meet its own requirements, and the lower the system reliability.

Table shows the effect of component allocation schemes on system reliability in different situations. We can see that the system reliability shown by the fixed allocation scheme and the optimized allocation scheme is different, and the optimal allocation scheme obtained by using the GA will significantly improve the system reliability. For example, in the first experiment, it is assumed that there is no performance loss during transmission. When the component



VIII CONCLUSION

Based on the practical engineering system, this paper proposes a multi-state system that considers multi-level performance sharing and transmission loss. Different from the previous research on system reliability with common bus performance sharing, the system model established in this paper has universal applicability and can calculate the reliability of any layer of system in practical application. In this system, there is a common bus sharing performance in each layer of subsystems. All lower-layer subsystems connected to a common bus can share performance through this common bus to meet each other's performance requirements. However, each common bus has its transmission capacity limit. If the total amount of shared performance exceeds the transmission capacity limit, the system will fail. In addition, we assume that there are two transmission modes. If the loss rate in the transmission process is low, the amount of loss in the transmission process is ignored. If the loss rate in the transmission process is high, the loss rate needs to be taken into account. As a result, we established a system reliability evaluation model with multi-level performance sharing by using UGF technique, and analyzed the effect of different parameters on system reliability. Then, we used GA to optimize the allocation of components in the system. Finally, it is proved by the above numerical experiments that these methods can significantly improve the overall reliability of the multi-layer system, including improving the performance of components, reducing the performance requirements of component groups, increasing the transmission capacity of the common bus, reducing the loss rate of transmission, and optimizing the allocation of components in the system.

In the future research, this study can be expanded in the following aspects. First of all, in this paper, the system failure is only affected by the internal transmission capacity limitation, and other failure modes and external effects are not considered. Secondly, this paper assumes that the transmission capacity of the common bus is limited to a constant. In the future, it can be considered that the transmission capacity will also be randomly distributed. Finally, this paper only considers a transmission loss mode, that is, the amount of transmission loss is proportional to the total amount of transmission performance, and the influence of transmission distance can be taken into account in the future.

REFERENCES

[1] K. Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. London, U.K.: Yale Univ. Press, 2021.

[2] D. Garcia, "Lethal artificial intelligence and change: The future of international peace and security," Int. Stud. Rev., vol. 20, no. 2, pp. 334– 341, Jun. 2018, doi: 10.1093/isr/viy029.

[3] T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, "Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature," Energies, vol. 13, no. 6, p. 1473, Mar. 2020, doi: 10.3390/en13061473.

[4] I. van Engelshoven. (Oct. 18, 2019). Speech by Minister Van Engelshoven on Artificial Intelligence at UNESCO, on October the 18th in Paris. Government of The Netherlands. Accessed: Apr. 15, 2021. [Online]. Available: https://www.government.nl/documents/speeches/2019/ 10/18/speech-by-minister-van-engelshoven-on-artificial-intelligenceatunesco

[5] O. Osoba and W. Welser IV, The Risks of Artificial Intelligence to Security and the Future of Work. Santa Monica, CA, USA: RAND Corporation, 2017, doi: 10.7249/PE237.

[6] D. Patel, Y. Shah, N. Thakkar, K. Shah, and M. Shah, "Implementation of artificial intelligence techniques for cancer detection," Augmented Hum. Res., vol. 5, no. 1, Dec. 2020, doi: 10.1007/s41133-019-0024-3.

[7] A. Rodríguez-Ruiz, E. Krupinski, J.-J. Mordang, K. Schilling, S. H. HeywangKöbrunner, I. Sechopoulos, and R. M. Mann, ‘‘Detection of breast cancer with mammography: Effect of an artificial intelligence support system,’’ Radiology, vol. 290, no. 2, pp. 305–314, Feb. 2019, doi: 10.1148/radiol.2018181371.

[8] J. Furman and R. Seamans, ‘‘AI and the economy,’’ Nat. Bur. Econ. Res., NBER, Cambridge, MA, USA, Work. Paper, 2018, doi: 10.3386/w24689.

[9] D. R. Coats, Worldwide Threat Assessment of the U.S. Intelligence Community. New York, NY, USA, 2017, p. 32.

[10] L. Floridi, ‘‘Soft ethics: Its application to the general data protection regulation and its dual advantage,’’ Philosophy Technol., vol. 31, no. 2, pp. 163–167, Jun. 2018, doi: 10.1007/s13347-018-0315-5.

[11] P. S. Chauhan and N. Kshetri, ‘‘2021 state of the practice in data privacy and security,’’ Computer, vol. 54, no. 8, pp. 125–132, Aug. 2021, doi: 10.1109/MC.2021.3083916.

[12] S. Gordon and R. Ford, ‘‘On the definition and classification of cybercrime,’’ J. Comput. Virol., vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/s11416-006-0015-z.

[13] Cybercrime. United Nations: Office Drugs. Accessed: May 19, 2021. http://www.unodc.org/unodc/en/cybercrime/index.html

[14] M. Brundage, S. Avin, J. Clark, and H. Toner, ‘‘The malicious use of artificial intelligence: Forecasting, prevention, and mitigation,’’ 2018, arXiv:1802.07228.

[15] T. C. King, N. Aggarwal, M. Taddeo, and L. Floridi, ‘‘Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions,’’ Sci. Eng. Ethics, vol. 26, no. 1, pp. 89–120, Feb. 2020, doi: 10.1007/s11948-018-00081-0.

[16] V. Ciancaglini, ‘‘Malicious uses and abuses of artificial intelligence,’’ in Trend Micro Research; United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol’s European Cybercrime Centre (EC3), Nov. 2020. [Online]. Available: https://www.europol.europa.eu/ publications-documents/malicious-uses-and-abuses-ofartificialintelligence

[17] K. D. Fiedler, V. Grover, and J. T. C. Teng, ‘‘An empirically derived taxonomy of information technology structure and its relationship to organizational structure,’’ J Manage. Inf. Syst., vol. 13, pp. 9–34, Jun. 1996, doi: 10.1080/07421222.1996.11518110.

[18] N. Bostrom, ‘‘Information hazards: A typology of potential harms from knowledge,’’ Rev. Contemp. Philosophy, vol. 10, pp. 44–79, May 2011.

[19] W. B. Carper and W. E. Snizek, ‘‘The nature and types of organizational taxonomies: An overview,’’ Acad. Manage. Rev., vol. 5, no. 1, pp. 65–75, Jan. 1980.

[20] (Apr. 21, 2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act. European Commission. Accessed: May 19, 2021. [Online]. Available: https://digitalstrategy.ec.europa.eu/en/library/proposal-regulationlaying-downharmonised-rules-artificial-intelligence-artificialintelligence

[21] Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act—Annexes to the Proposal. European Commission. Accessed: May 19, 2021. [Online].

[22] N. Akdemir and C. J. Lawless, ‘‘Exploring the human factor in cyberenabled and cyber-dependent crime victimisation: A lifestyle routine activities approach,’’ Internet Res., vol. 30, no. 6, pp. 1665–1687, Jun. 2020, doi: 10.1108/INTR-10-2019-0400.

[23] P. N. Grabosky, ‘‘Virtual criminality: Old wine in new bottles?’’ Social Legal Stud., vol. 10, no. 2, pp. 243–249, Jun. 2001, doi: 10.1177/a017405.

[24] B. Hibbard, Ethical Artificial Intelligence, 1st ed. Madison, WI, USA, 2015

[25] D. G. Johnson and M. Verdicchio, ‘‘Reframing AI discourse,’’ Minds Mach., vol. 27, no. 4, pp. 575–590, Dec. 2017, doi: 10.1007/s11023- 0179417-6.

[26] R. V. Yampolskiy, ‘‘Taxonomy of pathways to dangerous AI,’’ Phoenix, AZ, USA, Tech. Rep., Feb. 2016, pp. 143–148.

[27] A. Guterres. (May 2020). Protection of Civilians in Armed Conflict. United Nations, S/2020/366. Accessed: Jun. 2, 2020. [Online]. Available: https://undocs.org/en/S/2020/366

[28] E. Zouave, T. Gustafsson, M. Bruce, K. Colde, M. Jaitner, and I. Rodhe, ‘‘Artificially intelligent cyberattacks,’’ Swedish Defence Research Agency, FOI, Tech. Rep. FOI-R–4947-SE, Mar. 2020.

[29] J. Luo, T. Hong, and S.-C. Fang, ‘‘Benchmarking robustness of load forecasting models under data integrity attacks,’’ Int. J. Forecasting, vol. 34, no. 1, pp. 89–104, Jan. 2018, doi: 10.1016/j.ijforecast.2017.08.004.

[30] A. Kurakin, I. Goodfellow, and S. Bengio, ‘‘Adversarial machine learning at scale,’’ 2016, arXiv:1611.01236. [31] I. J. Goodfellow, J. Shlens, and C. Szegedy, ‘‘Explaining and harnessing adversarial examples,’’ 2014, arXiv:1412.6572.

[32] A. Kurakin, I. Goodfellow, and S. Bengio, ‘‘Adversarial examples in the physical world,’’ 2016, arXiv:1607.02533.

[33] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, ‘‘Manipulating machine learning: Poisoning attacks and countermeasures for regression learning,’’ in Proc. IEEE Symp. Secur. Privacy (SP), San Francisco, CA, USA, May 2018, pp. 19–35, doi: 10.1109/SP.2018.00057.

[34] O. Schwartz, ‘‘In 2016, Microsoft’s racist chatbot revealed the dangers of online conversation,’’ IEEE Spectr., to be published. Accessed: Apr. 13, 2021. [Online]. Available: https://spectrum.ieee.org/techtalk/artificialintelligence/machine-learning/in-2016-microsofts-racistchatbotrevealed-the-dangers-of-online-conversation

[35] T. Zemčík, ‘‘Failure of chatbot tay was evil, ugliness and uselessness in its nature or do we judge it through cognitive shortcuts and biases?’’ AI Soc., vol. 36, no. 1, pp. 361–367, Mar. 2021, doi: 10.1007/s00146- 02001053-4.

[36] P. Lee. (Mar. 25, 2016). Learning from Tay’s Introduction. Microsoft Blog. Accessed: Apr. 30, 2021. [Online]. Available: https://blogs. microsoft.com/blog/2016/03/25/learning-tays-introduction/

[37] N. Baracaldo, B. Chen, H. Ludwig, and J. A. Safavi, ‘‘Mitigating poisoning attacks on machine learning models: A data provenance based approach,’’ in Proc. 10th ACM Workshop Artif. Intell. Secur., Dallas, TX, USA, Nov. 2017, pp. 103–110, doi: 10.1145/3128572.3140450.

[38] T. Gu, B. Dolan-Gavitt, and S. Garg, ‘‘BadNets: Identifying vulnerabilities in the machine learning model supply chain,’’ 2017, arXiv:1708.06733.

[39] N. Carlini, C. Liu, Ú. Erlingsson, J. Kos, and D. Song, ‘‘The secret sharer: Evaluating and testing unintended memorization in neural networks,’’ 2018, arXiv:1802.08232.

[40] M. X. Chen, B. N. Lee, G. Bansal, Y. Cao, S. Zhang, J. Lu, J. Tsay, Y. Wang, A. M. Dai, Z. Chen, T. Sohn, and Y. Wu, ‘‘Gmail smart compose: Real-time assisted writing,’’ in Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Anchorage AK USA, Jul. 2019, pp. 2287–2295, doi: 10.1145/3292500.3330723.

[41] G. Scopino, AlgoBotsandtheLaw:Technology,Automation,andtheRegulation of Futures and Other Derivatives. Cambridge, U.K.: Cambridge Univ. Press,2020.

[42] T. C. W. Lin, ‘‘The new market manipulation,’’ Emory Law J., vol. 66, pp. 1253–1314, Jul. 2017.

[43] D. Wiener-Bronner. (Feb. 5, 2018). How the Dow Fell 800 Points in 10 Minutes. CNNMoney. Accessed: Jun. 24, 2021. [Online]. Available: https://money.cnn.com/2018/02/05/news/companies/dow-800- points10-minutes/index.html

[44] K. Martin. (May 7, 2020). Flash Crash—The Trading Savant Who CrashedtheU.S.StockMarket. Financial Times. Accessed: Apr. 14, 2021. [Online]. Available: https://www.ft.com/content/5ca93932-8de7- 11eaa8ec-961a33ba80aa

[45] S. N. Lynch and D. Miedema. (Apr. 22, 2015). U.K. Speed Trader Arrested Over Role in 2010. Flash Crash. Reuters, Washington, DC, USA. Accessed: Apr. 14, 2021. [Online]. Available: https://www.reuters.com/article/us-usa-security-fraud-idUSKBN0NC21220150422

[46] R. Wigglesworth. (Jan. 9, 2019). Volatility: How ‘algos’ Changed Rhythm Market. Financial Times. Accessed: Jun. 26, 2021. [Online]. Available: https://www-ft-com/content/fdc1c064-1142-11e9-a581-4ff78404524e

[47] A. Zwitter. (Jul. 27, 2017). The Artificial Intelligence Arms Race. Policy Forum. Accessed: Apr. 12, 2021. [Online]. Available: https://www. policyforum.net/artificial-intelligence-arms-race/

[48] J. Cox. (Feb. 16, 2018). The Stock Market Correction Two Weeks Later: How it Happened, and if it Can Happen Again. CNBC. Accessed: Jun. 24, 2021. [Online]. Available: https://www.cnbc.com/2018/02/16/the-stock-market-correction-two-weeks-later.html

[49] Y. Yadav, ‘‘The failure of liability in modern markets,’’ Virginia Law Rev.,

[50] R. Webster, J. Rabin, L. Simon, and F. Jurie, ‘‘This person (Probably) Exists. Identity membership attacks against GAN generated faces,’’ 2021, arXiv:2107.06018.

[51] H. Hu, Z. Salcic, L. Sun, G. Dobbie, P. S. Yu, and X. Zhang, ‘‘Membership inference attacks on machine learning: A survey,’’ 2021, arXiv:2103.07853.

[52] F. Mouton, L. Leenen, and H. S. Venter, ‘‘Social engineering attack examples, templates and scenarios,’’ Comput. Secur., vol. 59, pp. 186– 209, Jun. 2016, doi: 10.1016/j.cose.2016.03.004.

[53] C. Freitas, F. Benevenuto, S. Ghosh, and A. Veloso, ‘‘Reverse engineering socialbot infiltration strategies in Twitter,’’ in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining, Paris, France, Aug. 2015, pp. 25–32, doi: 10.1145/2808797.2809292.

[54] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, ‘‘Design and analysis of a social botnet,’’ Comput. Netw., vol. 57, no. 2, pp. 556–578, Feb. 2013, doi: 10.1016/j.comnet.2012.06.006.

[55] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, ‘‘The rise of social bots,’’ Commun. ACM, vol. 59, no. 7, pp. 96–104, Jul. 2016, doi: 10.1145/2818717.

[56] S. Rossi. (Dec. 15, 2007). Beware the CyberLover that Steals Personal Data. PCWorld. Accessed: May 11, 2020. [Online]. Available: https://www.pcworld.com/article/140507/article.html

[57] J. Seymour and P. Tully. (2016). Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us16Seymour-Tully-Weaponizing-Data-Science-For-Social-EngineeringAutomated-E2E-Spear-Phishing-On-Twitter-wp.pdf

[58] A. Bessi and E. Ferrara, ‘‘Social bots distort the 2016 U.S. Presidential election online discussion,’’ 1st Monday, vol. 21, no. 11, Nov. 2016.

[59] G. P. Nobre, J. M. Almeida, and C. H. G. Ferreira, ‘‘Caracterização de bots no Twitter durante as eleições presidenciais no Brasil em 2018,’’ in Anais do VIII Brazilian Workshop Social Netw. Anal. Mining (BraSNAM), Jul. 2019, pp. 107–118, doi: 10.5753/brasnam.2019.6553

[60] M. Kovic, A. Rauchfleisch, M. Sele, and C. Caspar, ‘‘Digital astroturfing in politics: Definition, typology, and countermeasures,’’ Stud. Commun. Sci., vol. 18, no. 1, Nov. 2018, doi: 10.24434/j.scoms.2018. 01.005.

[61] S. Mahbub, E. Pardede, A. S. M. Kayes, and W. Rahayu, ‘‘Controlling astroturfing on the Internet: A survey on detection techniques and research challenges,’’ Int. J. Web Grid Services, vol. 15, no. 2, p. 139, 2019, doi: 10.1504/IJWGS.2019.099561.

[62] F. B. Keller, D. Schoch, S. Stier, and J. Yang, ‘‘Political astroturfing on Twitter: How to coordinate a disinformation campaign,’’ Political Commun., vol. 37, no. 2, pp. 256–280, Mar. 2020, doi: 10.1080/10584609.2019.1661888.

[63] A. Zwitter. (Jun. 12, 2016). The Impact of Big Data of International Affairs. Clingendael Spectator. Accessed: Apr. 7, 2021. [Online]. Available: https://spectator.clingendael.org/en/publication/impactbigdata-international-affairs

[64] I. Lapowsky. (Nov. 28, 2017). How Bots Broke the FCC’s Public Comment System. Wired. Accessed: Apr. 8, 2021. [Online]. Available: https://www.wired.com/story/bots-broke-fcc-public-comment-system/

[65] C. Thuen. (Oct. 2, 2017). Discovering Truth Through Lies on the Internet—FCC Comments Analyzed. Gravwell. Accessed: Apr. 8, 2021. [Online]. Available: https://www.gravwell.io/blog/discoveringtruththrough-lies-on-the-internet-fcc-comments-analyzed

[66] V. Bakir, ‘‘Psychological operations in digital political campaigns: Assessing Cambridge analytica’s psychographic profiling and targeting,’’ Frontiers Commun., vol. 5, p. 67, Sep. 2020, doi: 10.3389/fcomm.2020.00067.

[67] J. Habgood-Coote, ‘‘Stop talking about fake news!’’ Inquiry, vol. 62, nos. 9–10, pp. 1033–1065, Nov. 2019, doi: 10.1080/0020174X.2018.1508363.

[68] M. Sullivan. (Jan. 8, 2017). It’s Time to Retire the Tainted Term. Fake News, The Washington Post. Accessed: Apr. 29, 2021. [Online]. Available: https://www.washingtonpost.com/lifestyle/style/its-time-toretire-thetainted-term-fake-news/2017/01/06/a5a7516c-d375-11e6- 945a-76f69a399dd5_story.html

[69] E. Zuckerman. (Jan. 31, 2017). Stop Saying ‘Fake News’. It’s Not Helping. Ethan Zuckerman. Accessed: Apr. 29, 2021. [Online]. Available: https://ethanzuckerman.com/2017/01/30/stop-saying-fakenews-itsnot-helping/

[70] S. Alonso García, G. Gómez García, M. Sanz Prieto, A. J. Moreno Guerrero, and C. Rodríguez Jiménez, ‘‘The impact of term fake news on the scientific community. Scientific performance and mapping in web of science,’’ Social Sci., vol. 9, no. 5, p. 73, May 2020, doi: 10.3390/socsci9050073.

[71] J. Pepp, E. Michaelson, and R. Sterken, ‘‘Why we should keep talking about fake news,’’ Inquiry, vol. 65, no. 4, pp. 471–487, Nov. 2019, doi: 10.1080/0020174X.2019.1685231.

[72] S. O. Oyeyemi, E. Gabarron, and R. Wynn, ‘‘Ebola, Twitter, and misinformation: A dangerous combination?’’ BMJ, vol. 349, pp. g6178– g6178, Oct. 2014, doi: 10.1136/bmj.g6178.

[73] J. Roozenbeek, C. R. Schneider, S. Dryhurst, J. Kerr, A. L. J. Freeman, G. Recchia, A. M. van der Bles, and S. van der Linden, ‘‘Susceptibility to misinformation about COVID-19 around the world,’’ Roy. Soc. Open Sci., vol. 7, no. 10, Oct. 2020, Art. no. 201199, doi: 10.1098/rsos.201199.

[74] W. L. Bennett and S. Livingston, ‘‘The disinformation order: Disruptive communication and the decline of democratic institutions,’’ Eur. J. Commun., vol. 33, no. 2, pp. 122–139, Apr. 2018, doi: 10.1177/0267323118760317.

[75] C. Machado, B. Kira, V. Narayanan, B. Kollanyi, and P. Howard, ‘‘A study of misinformation in WhatsApp groups with a focus on the Brazilian presidential Elections,’’ in Proc. Companion Proc. World Wide Web Conf., San Francisco, CA, USA, May 2019, pp. 1013–1019, doi: 10.1145/3308560.3316738.

[76] B. Wilder and Y. Vorobeychik, ‘‘Defending elections against malicious spread of misinformation,’’ in Proc. AAAI, vol. 33, Jul. 2019, pp. 2213– 2220, doi: 10.1609/aaai.v33i01.33012213.

[77] P. Nemitz, ‘‘Constitutional democracy and technology in the age of artificial intelligence,’’ Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci., vol. 376, no. 2133, Nov. 2018, Art. no. 20180089, doi: 10.1098/rsta.2018.0089.

[78] L. Floridi and M. Chiriatti, ‘‘GPT-3: Its nature, scope, limits, and consequences,’’ Minds Mach., vol. 30, pp. 681–694, Nov. 2020, doi: 10.1007/s11023-020-09548-1.

[79] K. McGuffie and A. Newhouse, ‘‘The radicalization risks of GPT-3 and advanced neural language models,’’ 2020, arXiv:2009.06807.

[80] Wordflow AI Articles. Accessed: Apr.

[81] R. Leyva and C. Beckett, ‘‘Testing and unpacking the effects of digital fake news: On presidential candidate evaluations and voter support,’’ AI Soc., vol. 35, no. 4, pp. 969–980, Dec. 2020, doi: 10.1007/s00146-02000980- 6

[82] S. M. Jones-Jang, T. Mortensen, and J. Liu, ‘‘Does media literacy help identification of fake news? Information literacy helps, but other literacies don’t,’’ Amer. Behav. Scientist, vol. 65, no. 2, pp. 371–388, Feb. 2021, doi: 10.1177/0002764219869406.

[83] Association for College and Research Libraries. (2016). Framework for Information Literacy for Higher Education. Accessed: Jun. 29, 2021. [Online]. Available: https://www-ala-org.proxyub.rug.nl/acrl/standards/ilframework

[84] O. J. Gstrein, ‘‘Right to be forgotten: European data imperialism, national privilege, or universal human right?’’ Rev. Eur. Administ. Law, vol. 13, no. 1, pp. 125–152, May 2020, doi: 10.7590/187479820X15881424928426.

[85] H. Allcott and M. Gentzkow, ‘‘Social media and fake news in the 2016 election,’’ J. Econ. Perspect., vol. 31, no. 2, pp. 211–236, May 2017, doi: 10.1257/jep.31.2.211.

[86] C. Shah. (Mar. 10, 2021). It’s Not Just a Social Media Problem—How Search Engines Spread Misinformation. The Conversation. Accessed: Jun. 29, 2021. [Online]. Available: http://theconversation.com/itsnotjust-a-social-media-problem-how-search-enginesspreadmisinformation-152155

[87] C. Arun, ‘‘Facebook’s faces,’’ in Forthcoming Harvard Law Review Forum, vol. 135. Mar. 2021, doi: 10.2139/ssrn.3805210.

[88] G. De Gregorio, ‘‘Democratising online content moderation: A constitutional framework,’’ Comput. Law Secur. Rev., vol. 36, Apr. 2020, Art. no. 105374, doi: 10.1016/j.clsr.2019.105374.

[89] R. T. Garcia. (Jun. 19, 2020). Anonymous Twitter Accounts in Brazil are Pressuring Advertisers to Drop Conservative Media Campaigns. Insider. Accessed: Jun. 29, 2021. [Online]. Available: https://www.insider.com/sleeping-giants-brasil-borrowing-us-tacticforfighting-misinformation-2020-6

[90] J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Niessner, ‘‘Face2Face: Real-time face capture and reenactment of RGB videos,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016, pp. 2387–2395.

[91] M. Westerlund, ‘‘The emergence of deepfake technology: A review,’’ Technol. Innov. Manage. Rev., vol. 9, no. 11, pp. 39–52, Jan. 2019, doi: 10.22215/timreview/1282.

[92] T. Greene. (Apr. 21, 2020). Watch: Fake Elon Musk Zoom-Bombs Meeting Using Real-Time Deepfake AI. Neural | The Next Web. Accessed: Apr. 7, 2021. [Online]. Available: https://thenextweb.com/ neural/2020/04/21/watch-fake-elon-musk-zoom-bombs-meetingusingreal-time-deepfake-ai/

[93] L. Guarnera, O. Giudice, C. Nastasi, and S. Battiato, ‘‘Preliminary forensics analysis of DeepFake images,’’ 2020, arXiv:2004.12626.

[94] M.-H. Maras and A. Alexandrou, ‘‘Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos,’’ Int. J. Evidence Proof, vol. 23, no. 3, pp. 255–

[95] D. O’Sullivan. (Aug. 10, 2019). The Democratic Party Deepfaked Its Own Chairman to Highlight 2020 Concerns. CNN. Accessed: May 11, 2020. [Online]. Available: https://www.cnn.com/2019/08/09/ tech/deepfake-tom-perez-dnc-defcon/index.html

[96] D. Fonseca. (Jan. 18, 2021). BrunoSartori:OReiDASDeepfakes. Revista Trip. Accessed: Jun. 28, 2021. [Online]. Available: https://revistatrip. uol.com.br/trip/webstories/bruno-sartori-o-rei-das-deepfakes

[97] J. Compton, ‘‘Inoculation theory,’’ in SAGE Handbook of Persuasion: Developments in Theory and Practice. Newbury Park, CA, USA: Sage, 2012, pp. 220–236, doi: 10.4135/9781452218410.n14.

[98] W. J. McGuire, ‘‘Inducing resistance to persuasion: Some contemporary approaches,’’ in Advances in Experimental Social Psychology, vol. 1, L. Berkowitz, Ed. New York, NY, USA: Academic, 1964, pp. 191–229.

[99] D. Guera and E. J. Delp, ‘‘Deepfake video detection using recurrent neural networks,’’ in Proc. 15th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), Auckland, New Zealand, Nov. 2018, pp. 1–6, doi: 10.1109/AVSS.2018.8639163.

[100] R. Chesney and D. K. Citron, ‘‘Deep fakes: A looming challenge for privacy, democracy, and national security,’’ SSRN J., pp. 1753–1820, 2018, doi: 10.2139/ssrn.3213954.

[101] V. Elliott and M. Tobin. (Jan. 10, 2022). China Steps up Efforts to Ban Deepfakes. Will it work? Rest World. Accessed: Mar. 1, 2022. [Online]. Available: https://restofworld.org/2022/china-steps-upeffortsto-ban-deepfakes/

[102] K. Zetter. (Nov. 19, 2010). Wiseguys Plead Guilty in Ticketmaster Captcha Case. Wired. Accessed: Jun. 2, 2020. [Online]. Available: https://www.wired.com/2010/11/wiseguys-plead-guilty/

[103] K. Trieu and Y. Yang. (2018). Artificial Intelligence-Based Password Brute Force Attacks. [Online]. Available: http://aisel.aisnet.org/ mwais2018/39

[104] D. Gibert, C. Mateu, and J. Planes, ‘‘The rise of machine learning for detection and classification of malware: Research developments, trends and challenges,’’ J. Netw. Comput. Appl., vol. 153, Mar. 2020, Art. no. 102526, doi: 10.1016/j.jnca.2019.102526.

[105] AV-TEST. (2021). Malware Statistics & Trends Report. AV-TEST: The Independ. IT-Security Inst. Accessed: Jun. 22, 2021. [Online]. Available: https://www.av-test.org/en/statistics/malware/

[106] (2018). DeepLocker—Concealing Targeted Attacks With AI Locksmithing. Black Hat USA. Accessed: Apr. 22, 2021. [Online]. Available: https://www.blackhat.com/us18/briefings/schedule/#deeplocker— concealing-targeted-attacks-withai-

locksmithing-11549262, Jul. 2019, doi: 10.1177/1365712718807226. [95] D. O'Sullivan. (Aug. 10, 2019). The Democratic Party Deepfaked Its Own Chairman to Highlight 2020 Concerns. CNN. Accessed:

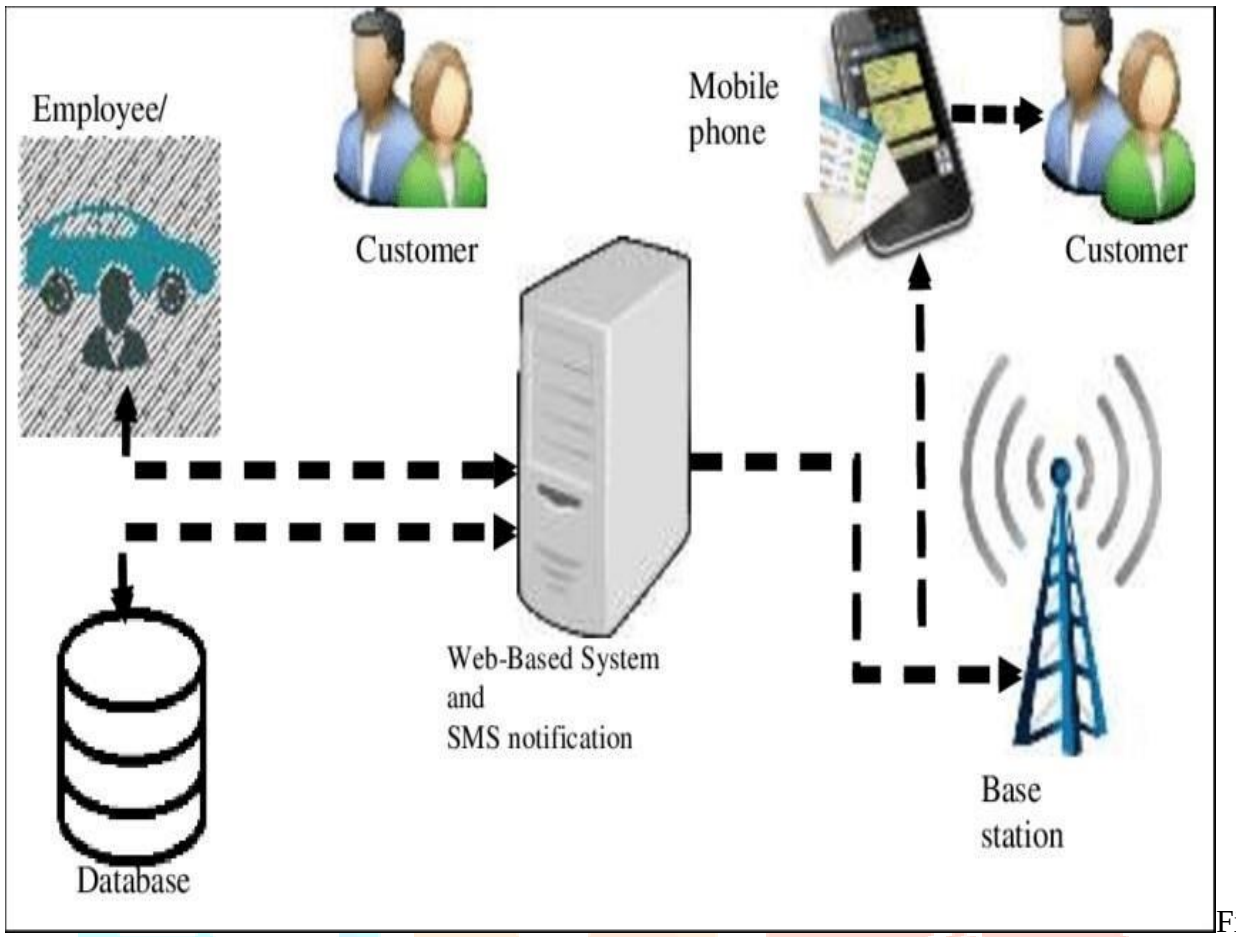


Fig: Architecture of Online Rental Things

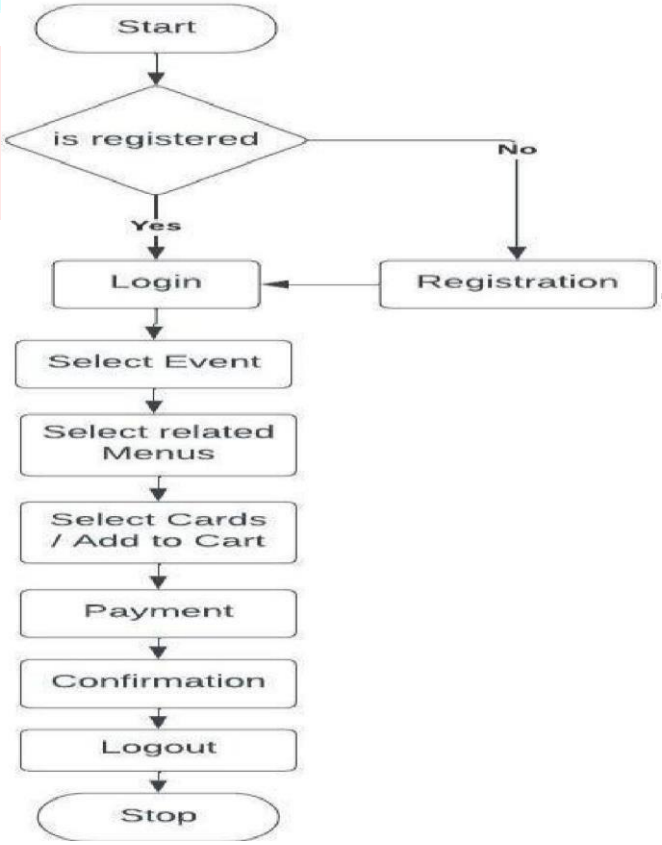
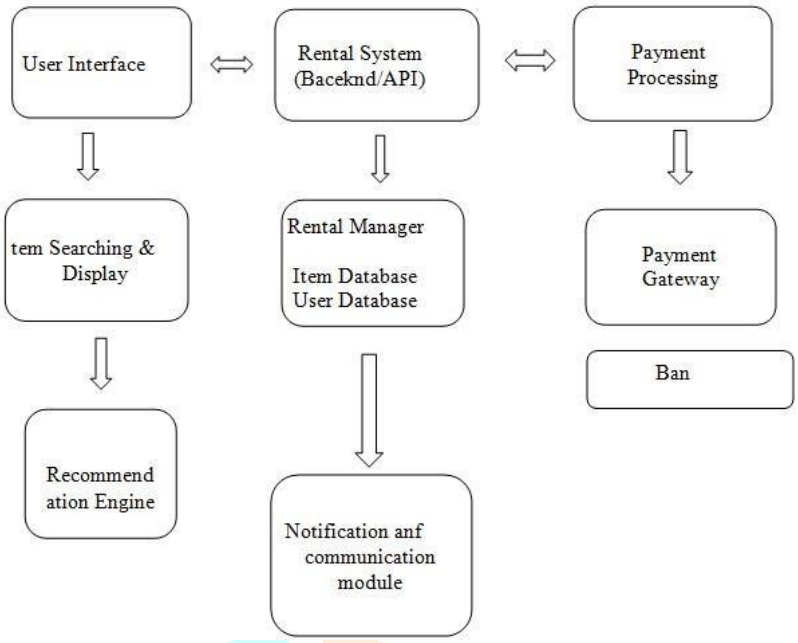


Fig: System Diagram for Rental Things

Creating a system architecture diagram typically involves visual representation using various symbols and shapes. Here's a simplified textual representation of the components and their interactions for a rental system:



Components:

- User Interface: Represents the front-end where users interact with the system.
- Item Search & Display: Handles user queries, displays items, and may incorporate recommendation engine results.
- Recommendation Engine: Provides personalized recommendations based on user preferences and item popularity.
- Rental System (Backend/APIs): Manages the core logic of the rental system, including rental requests, reservations, agreements, and return processing.
- Rental Manager: Coordinates rental-related operations, communicates with item and user databases.
- Item Database: Stores information about available items, their status, and rental history.
- User Database: Manages user profiles, rental history, and eligibility criteria.
- Payment Processing: Interacts with a payment gateway for secure transaction processing.
- Payment Gateway: Handles payment transactions securely, communicating with banking APIs.
- Notification and Communication Module: Sends notifications to users about rental confirmations, return deadlines, and other updates

This is a high-level representation, and depending on the specific requirements, you might need to include additional components, such as a logging system, security measures, and monitoring tools. Each box in the diagram represents a functional module or service, and the arrows indicate the flow of data or interactions between them.

VI. IMPLEMENTATION AND ALGORITHMS

A. Implementation:

The core functionality of the system involves tracking crops through the supply chain securely. This is achieved through the following steps:

1. User Registration: At the beginning of the Ecommerce website, each user is registered on the website with a unique identifier, including relevant details such as user name, password.

2. Data Transmission: After collection, data is transmitted to a firebase. This transmission may involve wireless technologies, such as Wi-Fi, cellular networks, or satellite connections, depending on the location and available infrastructure.
3. Data Storage: Data is securely stored on cloud
4. Data Processing and Analysis: The stored data is processed and analysed to derive valuable insights. Data processing may involve analytics, machine learning, and artificial intelligence techniques to identify trends, patterns, and anomalies in the Rental products.
5. Products Recommendation: Products Recommendation algorithms are used to Recommendation products to the users.
6. Payment Gateway: System will provide transaction methods like online, COD etc.

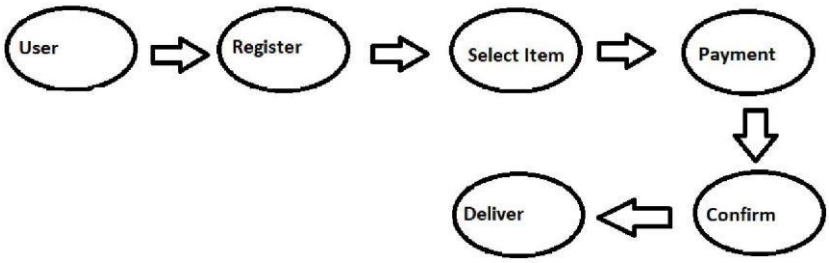


Fig. 3. Data Flow Diagram

B. Algorithms:

Here's a step-by-step theoretical overview of a simplified algorithm for managing rentals:

1. Item Representation: Each rental item is represented in a system, and relevant information such as item ID, type, availability status, and rental history is stored.
2. User Interaction: Users can interact with the system to search for available items, request rentals, and return rented items.
3. Search and Recommendation: Users can search for items based on criteria like type, availability, or other attributes. A recommendation system may suggest items based on user preferences or popular choices.
4. Rental Request: Users initiate a rental request for a selected item. The system checks the item's availability and user eligibility (e.g., account status, rental history).
5. Reservation: If the item is available and the user is eligible, the system reserves the item for the user, marking it as temporarily unavailable to others.
6. Rental Agreement: Users review and agree to the rental terms, including rental duration, fees, and any conditions. The system records the agreement.
7. Payment Processing: Users provide payment information, and the system processes the rental fees. This step may involve secure payment gateways.
8. Notification: Users receive confirmation of their rental along with details such as pickup/delivery instructions and return deadlines.
9. Item Pickup/Delivery: Users pick up the rented item or receive it through a delivery service. The system updates the item status to "rented."
10. Rental Period: The system monitors the rental period, notifying users of upcoming return deadlines and handling any extensions or early returns.
11. Return Request: Users initiate a return request through the system, indicating the item's condition.
12. Return Inspection: The system may conduct an inspection of the returned item, checking for damage or discrepancies from the initial condition.
13. Fee Calculation: Fees, if any (e.g., late fees or damage charges), are calculated based on the rental terms and item condition.
14. Transaction Completion: The rental transaction is completed. Users receive a summary of the transaction, including any additional charges or refunds.

15. Feedback and Ratings: Users may provide feedback and ratings for the rental experience and the rented item. This information can be used for future recommendations.

This step-by-step overview provides a high-level understanding of the rental process. Implementation details may vary based on the specific features and requirements of the rental system.

VII. DISCUSSION

AI techniques are increasingly deployed in different areas and for an increasing number of purposes. This brings both benefits and risks to society [14]. Among the risks are the use and abuse of AI systems with malicious intent. Even though the capabilities of AIenhanced technology might not always lead to more sophisticated attacks, they certainly have the potential to increase scale and reach. Cybercriminals will progressively integrate AI techniques and the use of AI systems in their plans.

The risks presented in our overview are especially challenging when cybercriminals exploit systems during periods of societal instability. This is facilitated during the COVID-19 pandemic, which caused a growth in the number of people using online tools to work and socialize. The massive shift of social interaction to the online environment increased security vulnerabilities, which malicious actors already exploit at an alarming rate [126]. Not only were individuals and small businesses targeted; in fact, Interpol identified that cybercriminals focused on critical infrastructure, major corporations, and governments [127]. Given the potential impacts of such attacks, it is vital to consider and mitigate these risks.

Some of the issues presented in this overview have been discussed elsewhere [15], [16]. However, in addition to adding novel types of threats in our typology (e.g. Membership Inference Attacks) and providing salient examples, we also provided a different classification than previous works. We divide the attacks between (1) AI-Enabled/ AI-Enhanced attacks and (2) vulnerabilities of AI models. We submit that such separation is helpful because different strategies can alleviate the risks

Addressing challenges linked to vulnerabilities of AI models is highly dependent on the work of engineers and development teams. Developing robust AI systems is paramount. To this end, teams behind the development of algorithms should adhere to principles such as privacyby-design. Organizations, government bodies, and scholars are developing and fine-tuning impact assessment tools for AI systems [128]–[130]. Such tools help translate relevant principles (such as privacy, transparency and fairness [131]) into practical evaluations. Efforts to identify risks via impact assessments are already conducted for data protection compliance in many countries, and similar initiatives can be helpful to deal with the challenges presented by AI systems.

When discussing ways of dealing with the risks presented by AI-Enabled/AI-Enhanced attacks, more is needed in prevention/proactive measures and adequate response. Given that regulatory frameworks and governance mechanisms might not be formulated at the same pace of technological advancements, it is vital to act proactively to reduce the risks outlined in this paper. Instead of finding one overarching solution, different sectors of society could gradually identify initiatives that can help build more resilience and preparedness. Initiatives with local communities, such as promoting data and information literacy, reducing digital divide gaps, and creating campaigns to raise awareness on AI-related threats can be a staring point.

Finally, we wish to emphasize that when discussing the challengesposedbyAIsystems,oneshouldnotforgetthatt he possibilities are also limited. Some simple and easy tasks for humans (e.g., sensorimotor skills such as developing motor abilities through the senses) can be difficult or even impossible for computers to carry out. At the same time, some functions that are complex to humans can be quickly developed in AI systems (e.g., finding patterns in an extensive data set). This is the basis of what became known as Moravec's paradox: ''it is comparatively easy to make computers exhibit adultlevel performance in solving problems on intelligence tests of playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and

mobility" [132, p. 15]. Understanding the actual capabilities and limitations of emerging technologies such as AI is therefore critical for developing effective policies and strategies for living in a safer world.

VIII . CONCLUSION

In conclusion, developing an ecommerce website for our Smart Rental Application is here to make life easier for everyone. With this app, renting items and services becomes a breeze. We've put in a lot of effort to create something that's user-friendly and super convenient. Now, you can rent what you need, when you need it, and do it all with confidence.

In conclusion, the "Online Rental Things" project represents an innovative and promising solution to the challenges of underutilization of resources, inefficient access to items, and the growing demand for sustainability in our modern society. By facilitating the sharing of various items and resources through a user-friendly online platform, this project offers a range of advantages, including resource efficiency, cost savings, and community building.

However, it's important to acknowledge the potential limitations and challenges associated with such a venture These challenges include building user trust, ensuring the quality of items addressing regulatory concerns, and competing in a dynamic market

REFERENCES

[1] K. Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. London, U.K.: Yale Univ. Press, 2021.

[2] D. Garcia, ‘‘Lethal artificial intelligence and change: The future of international peace and security,’’ Int. Stud. Rev., vol. 20, no. 2, pp. 334– 341, Jun. 2018, doi: 10.1093/isr/viy029.

[3] T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, ‘‘Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature,’’ Energies, vol. 13, no. 6, p. 1473, Mar. 2020, doi: 10.3390/en13061473.

[4] I. van Engelshoven. (Oct. 18, 2019). Speech by Minister Van Engelshoven on Artificial Intelligence at UNESCO, on October the 18th in Paris. Government of The Netherlands. Accessed: Apr. 15, 2021. [Online]. Available: https://www.government.nl/documents/speeches/2019/ 10/18/speech-by-minister-van-engelshoven-on-artificial-intelligenceatunesco

[5] O. Osoba and W. Welser IV, The Risks of Artificial Intelligence to Security and the Future of Work. Santa Monica, CA, USA: RAND Corporation, 2017, doi: 10.7249/PE237.

[6] D. Patel, Y. Shah, N. Thakkar, K. Shah, and M. Shah, ‘‘Implementation of artificial intelligence techniques for cancer detection,’’ Augmented Hum. Res., vol. 5, no. 1, Dec. 2020, doi: 10.1007/s41133-019-0024-3.

[7] A. Rodríguez-Ruiz, E. Krupinski, J.-J. Mordang, K. Schilling, S. H. HeywangKöbrunner, I. Sechopoulos, and R. M. Mann, ‘‘Detection of breast cancer with mammography: Effect of an artificial intelligence support system,’’ Radiology, vol. 290, no. 2, pp. 305–314, Feb. 2019, doi: 10.1148/radiol.2018181371.

[8] J. Furman and R. Seamans, ‘‘AI and the economy,’’ Nat. Bur. Econ. Res., NBER, Cambridge, MA, USA, Work. Paper, 2018, doi: 10.3386/w24689.

[9] D. R. Coats, Worldwide Threat Assessment of the U.S. Intelligence Community. New York, NY, USA, 2017, p. 32.

[10] L. Floridi, ‘‘Soft ethics: Its application to the general data protection regulation and its dual advantage,’’ Philosophy Technol., vol. 31, no. 2, pp. 163–167, Jun. 2018, doi: 10.1007/s13347-018-0315-5.

[11] P. S. Chauhan and N. Kshetri, ‘‘2021 state of the practice in data privacy and security,’’ Computer, vol. 54, no. 8, pp. 125–132, Aug. 2021, doi: 10.1109/MC.2021.3083916.

[12] S. Gordon and R. Ford, ‘‘On the definition and classification of cybercrime,’’ J. Comput. Virol., vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/s11416-006-0015-z.

[13] Cybercrime. United Nations: Office Drugs. Accessed: May 19, 2021. http://www.unodc.org/unodc/en/cybercrime/index.html

[14] M. Brundage, S. Avin, J. Clark, and H. Toner, ‘‘The malicious use of artificial intelligence: Forecasting, prevention, and mitigation,’’ 2018, arXiv:1802.07228.

[15] T. C. King, N. Aggarwal, M. Taddeo, and L. Floridi, ‘‘Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions,’’ Sci. Eng. Ethics, vol. 26, no. 1, pp. 89–120, Feb. 2020, doi: 10.1007/s11948-018-00081-0.

[16] V. Ciancaglini, ‘‘Malicious uses and abuses of artificial intelligence,’’ in Trend Micro Research; United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol’s European Cybercrime Centre (EC3), Nov. 2020. [Online]. Available: https://www.europol.europa.eu/ publications-documents/malicious-uses-and-abuses-ofartificialintelligence

[17] K. D. Fiedler, V. Grover, and J. T. C. Teng, ‘‘An empirically derived taxonomy of information technology structure and its relationship to organizational structure,’’ J Manage. Inf. Syst., vol. 13, pp. 9–34, Jun. 1996, doi: 10.1080/07421222.1996.11518110.

[18] N. Bostrom, ‘‘Information hazards: A typology of potential harms from knowledge,’’ Rev. Contemp. Philosophy, vol. 10, pp. 44–79, May 2011.

[19] W. B. Carper and W. E. Snizek, ‘‘The nature and types of organizational taxonomies: An overview,’’ Acad. Manage. Rev., vol. 5, no. 1, pp. 65–75, Jan. 1980.

[20] (Apr. 21, 2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act. European Commission. Accessed: May 19, 2021. [Online]. Available: https://digitalstrategy.ec.europa.eu/en/library/proposal-regulationlaying-downharmonised-rules-artificial-intelligence-artificialintelligence

[21] Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act—Annexes to the Proposal. European Commission. Accessed: May 19, 2021. [Online].

[22] N. Akdemir and C. J. Lawless, ‘‘Exploring the human factor in cyberenabled and cyber-dependent crime victimisation: A lifestyle routine activities approach,’’ Internet Res., vol. 30, no. 6, pp. 1665–1687, Jun. 2020, doi: 10.1108/INTR-10-2019-0400.

[23] P. N. Grabosky, ‘‘Virtual criminality: Old wine in new bottles?’’ Social Legal Stud., vol. 10, no. 2, pp. 243–249, Jun. 2001, doi: 10.1177/a017405.

[24] B. Hibbard, Ethical Artificial Intelligence, 1st ed. Madison, WI, USA, 2015

[25] D. G. Johnson and M. Verdicchio, ‘‘Reframing AI discourse,’’ Minds Mach., vol. 27, no. 4, pp. 575–590, Dec. 2017, doi: 10.1007/s11023- 0179417-6.

[26] R. V. Yampolskiy, ‘‘Taxonomy of pathways to dangerous AI,’’ Phoenix, AZ, USA, Tech. Rep., Feb. 2016, pp. 143–148.

[27] A. Guterres. (May 2020). Protection of Civilians in Armed Conflict. United Nations, S/2020/366. Accessed: Jun. 2, 2020. [Online]. Available: https://undocs.org/en/S/2020/366

[28] E. Zouave, T. Gustafsson, M. Bruce, K. Colde, M. Jaitner, and I. Rodhe, "Artificially intelligent cyberattacks," Swedish Defence Research Agency, FOI, Tech. Rep. FOI-R–4947-SE, Mar. 2020.

[29] J. Luo, T. Hong, and S.-C. Fang, "Benchmarking robustness of load forecasting models under data integrity attacks," Int. J. Forecasting, vol. 34, no. 1, pp. 89–104, Jan. 2018, doi: 10.1016/j.ijforecast.2017.08.004.

[30] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial machine learning at scale," 2016, arXiv:1611.01236. [31] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, arXiv:1412.6572.

[32] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," 2016, arXiv:1607.02533.

[33] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," in Proc. IEEE Symp. Secur. Privacy (SP), San Francisco, CA, USA, May 2018, pp. 19–35, doi: 10.1109/SP.2018.00057.

[34] O. Schwartz, "In 2016, Microsoft's racist chatbot revealed the dangers of online conversation," IEEE Spectr., to be published. Accessed: Apr. 13, 2021. [Online]. Available: https://spectrum.ieee.org/techtalk/artificialintelligence/machine-learning/in-2016-microsofts-racistchatbotrevealed-the-dangers-of-online-conversation

[35] T. Zemčík, "Failure of chatbot tay was evil, ugliness and uselessness in its nature or do we judge it through cognitive shortcuts and biases?" AI Soc., vol. 36, no. 1, pp. 361–367, Mar. 2021, doi: 10.1007/s00146- 02001053-4.

[36] P. Lee. (Mar. 25, 2016). Learning from Tay's Introduction. Microsoft Blog. Accessed: Apr. 30, 2021. [Online]. Available: https://blogs. microsoft.com/blog/2016/03/25/learning-tays-introduction/

[37] N. Baracaldo, B. Chen, H. Ludwig, and J. A. Safavi, "Mitigating poisoning attacks on machine learning models: A data provenance based approach," in Proc. 10th ACM Workshop Artif. Intell. Secur., Dallas, TX, USA, Nov. 2017, pp. 103–110, doi: 10.1145/3128572.3140450.

[38] T. Gu, B. Dolan-Gavitt, and S. Garg, "BadNets: Identifying vulnerabilities in the machine learning model supply chain," 2017, arXiv:1708.06733.

[39] N. Carlini, C. Liu, Ú. Erlingsson, J. Kos, and D. Song, "The secret sharer: Evaluating and testing unintended memorization in neural networks," 2018, arXiv:1802.08232.

[40] M. X. Chen, B. N. Lee, G. Bansal, Y. Cao, S. Zhang, J. Lu, J. Tsay, Y. Wang, A. M. Dai, Z. Chen, T. Sohn, and Y. Wu, "Gmail smart compose: Real-time assisted writing," in Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Anchorage AK USA, Jul. 2019, pp. 2287–2295, doi: 10.1145/3292500.3330723.

[41] G. Scopino, AlgoBotsandtheLaw:Technology,Automation,andtheRegulation of Futures and Other Derivatives. Cambridge, U.K.: Cambridge Univ. Press,2020.

[42] T. C. W. Lin, "The new market manipulation," Emory Law J., vol. 66, pp. 1253–1314, Jul. 2017.

[43] D. Wiener-Bronner. (Feb. 5, 2018). How the Dow Fell 800 Points in 10 Minutes. CNNMoney. Accessed: Jun. 24, 2021. [Online]. Available: https://money.cnn.com/2018/02/05/news/companies/dow-800- points10-minutes/index.html

[44] K. Martin. (May 7, 2020). Flash Crash—The Trading Savant Who CrashedtheU.S.StockMarket. Financial Times. Accessed: Apr. 14, 2021. [Online]. Available: https://www.ft.com/content/5ca93932-8de7- 11eaa8ec-961a33ba80aa

[45] S. N. Lynch and D. Miedema. (Apr. 22, 2015). U.K. Speed Trader Arrested Over Role in 2010. Flash Crash. Reuters, Washington, DC, USA. Accessed: Apr. 14, 2021. [Online]. Available: https://www.reuters. com/article/us-usa-security-fraud-idUSKBN0NC21220150422

[46] R. Wigglesworth. (Jan. 9, 2019). Volatility: How 'algos' Changed Rhythm Market. Financial Times. Accessed: Jun. 26, 2021. [Online]. Available: https://www-ft-com/content/fdc1c064-1142-11e9-a581-4ff78404524e

[47] A. Zwitter. (Jul. 27, 2017). The Artificial Intelligence Arms Race. Policy Forum. Accessed: Apr. 12, 2021. [Online]. Available: https://www. policyforum.net/artificial-intelligence-arms-race/

[48] J. Cox. (Feb. 16, 2018). The Stock Market Correction Two Weeks Later: How it Happened, and if it Can Happen Again. CNBC. Accessed: Jun. 24, 2021. [Online]. Available: https://www.cnbc.com/ 2018/02/16/the-stock-market-correction-two-weeks-later.html

[49] Y. Yadav, ''The failure of liability in modern markets,'' Virginia Law Rev.,

[50] R. Webster, J. Rabin, L. Simon, and F. Jurie, ''This person (Probably) Exists. Identity membership attacks against GAN generated faces,'' 2021, arXiv:2107.06018.

[51] H. Hu, Z. Salcic, L. Sun, G. Dobbie, P. S. Yu, and X. Zhang, ''Membership inference attacks on machine learning: A survey,'' 2021, arXiv:2103.07853.

[52] F. Mouton, L. Leenen, and H. S. Venter, ''Social engineering attack examples, templates and scenarios,'' Comput. Secur., vol. 59, pp. 186– 209, Jun. 2016, doi: 10.1016/j.cose.2016.03.004.

[53] C. Freitas, F. Benevenuto, S. Ghosh, and A. Veloso, ''Reverse engineering socialbot infiltration strategies in Twitter,'' in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining, Paris, France, Aug. 2015, pp. 25–32, doi: 10.1145/2808797.2809292.

[54] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, ''Design and analysis of a social botnet,'' Comput. Netw., vol. 57, no. 2, pp. 556–578, Feb. 2013, doi: 10.1016/j.comnet.2012.06.006.

[55] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, ''The rise of social bots,'' Commun. ACM, vol. 59, no. 7, pp. 96–104, Jul. 2016, doi: 10.1145/2818717.

[56] S. Rossi. (Dec. 15, 2007). Beware the CyberLover that Steals Personal Data. PCWorld. Accessed: May 11, 2020. [Online]. Available: https://www.pcworld.com/article/140507/article.html

[57] J. Seymour and P. Tully. (2016). Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us16Seymour-Tully-Weaponizing-Data-Science-For-Social-EngineeringAutomated-E2E-Spear-Phishing-On-Twitter-wp.pdf

[58] A. Bessi and E. Ferrara, ''Social bots distort the 2016 U.S. Presidential election online discussion,'' 1st Monday, vol. 21, no. 11, Nov. 2016.

[59] G. P. Nobre, J. M. Almeida, and C. H. G. Ferreira, ''Caracterização de bots no Twitter durante as eleições presidenciais no Brasil em 2018,'' in Anais do VIII Brazilian Workshop Social Netw. Anal. Mining (BraSNAM), Jul. 2019, pp. 107–118, doi: 10.5753/brasnam.2019.6553

[60] M. Kovic, A. Rauchfleisch, M. Sele, and C. Caspar, ''Digital astroturfing in politics: Definition, typology, and countermeasures,'' Stud. Commun. Sci., vol. 18, no. 1, Nov. 2018, doi: 10.24434/j.scoms.2018. 01.005.

[61] S. Mahbub, E. Pardede, A. S. M. Kayes, and W. Rahayu, ‘‘Controlling astroturfing on the Internet: A survey on detection techniques and research challenges,’’ Int. J. Web Grid Services, vol. 15, no. 2, p. 139, 2019, doi: 10.1504/IJWGS.2019.099561.

[62] F. B. Keller, D. Schoch, S. Stier, and J. Yang, ‘‘Political astroturfing on Twitter: How to coordinate a disinformation campaign,’’ Political Commun., vol. 37, no. 2, pp. 256–280, Mar. 2020, doi: 10.1080/10584609.2019.1661888.

[63] A. Zwitter. (Jun. 12, 2016). The Impact of Big Data of International Affairs. Clingendael Spectator. Accessed: Apr. 7, 2021. [Online]. Available: https://spectator.clingendael.org/en/publication/impactbigdata-international-affairs

[64] I. Lapowsky. (Nov. 28, 2017). How Bots Broke the FCC’s Public Comment System. Wired. Accessed: Apr. 8, 2021. [Online]. Available: https://www.wired.com/story/bots-broke-fcc-public-comment-system/

[65] C. Thuen. (Oct. 2, 2017). Discovering Truth Through Lies on the Internet—FCC Comments Analyzed. Gravwell. Accessed: Apr. 8, 2021. [Online]. Available: https://www.gravwell.io/blog/discoveringtruththrough-lies-on-the-internet-fcc-comments-analyzed

[66] V. Bakir, ‘‘Psychological operations in digital political campaigns: Assessing Cambridge analytica’s psychographic profiling and targeting,’’ Frontiers Commun., vol. 5, p. 67, Sep. 2020, doi: 10.3389/fcomm.2020.00067.

[67] J. Habgood-Coote, ‘‘Stop talking about fake news!’’ Inquiry, vol. 62, nos. 9–10, pp. 1033–1065, Nov. 2019, doi: 10.1080/0020174X.2018.1508363.

[68] M. Sullivan. (Jan. 8, 2017). It’s Time to Retire the Tainted Term. Fake News, The Washington Post. Accessed: Apr. 29, 2021. [Online]. Available: https://www.washingtonpost.com/lifestyle/style/its-time-toretire-thetainted-term-fake-news/2017/01/06/a5a7516c-d375-11e6- 945a-76f69a399dd5_story.html

[69] E. Zuckerman. (Jan. 31, 2017). Stop Saying ‘Fake News’. It’s Not Helping. Ethan Zuckerman. Accessed: Apr. 29, 2021. [Online]. Available: https://ethanzuckerman.com/2017/01/30/stop-saying-fakenews-itsnot-helping/

[70] S. Alonso García, G. Gómez García, M. Sanz Prieto, A. J. Moreno Guerrero, and C. Rodríguez Jiménez, ‘‘The impact of term fake news on the scientific community. Scientific performance and mapping in web of science,’’ Social Sci., vol. 9, no. 5, p. 73, May 2020, doi: 10.3390/socsci9050073.

[71] J. Pepp, E. Michaelson, and R. Sterken, ‘‘Why we should keep talking about fake news,’’ Inquiry, vol. 65, no. 4, pp. 471–487, Nov. 2019, doi: 10.1080/0020174X.2019.1685231.

[72] S. O. Oyeyemi, E. Gabarron, and R. Wynn, ‘‘Ebola, Twitter, and misinformation: A dangerous combination?’’ BMJ, vol. 349, pp. g6178– g6178, Oct. 2014, doi: 10.1136/bmj.g6178.

[73] J. Roozenbeek, C. R. Schneider, S. Dryhurst, J. Kerr, A. L. J. Freeman, G. Recchia, A. M. van der Bles, and S. van der Linden, ‘‘Susceptibility to misinformation about COVID-19 around the world,’’ Roy. Soc. Open Sci., vol. 7, no. 10, Oct. 2020, Art. no. 201199, doi: 10.1098/rsos.201199.

[74] W. L. Bennett and S. Livingston, ‘‘The disinformation order: Disruptive communication and the decline of democratic institutions,’’ Eur. J. Commun., vol. 33, no. 2, pp. 122–139, Apr. 2018, doi: 10.1177/0267323118760317.

[75] C. Machado, B. Kira, V. Narayanan, B. Kollanyi, and P. Howard, ‘‘A study of misinformation in WhatsApp groups with a focus on the Brazilian presidential Elections,’’ in Proc. Companion

Proc. World Wide Web Conf., San Francisco, CA, USA, May 2019, pp. 1013–1019, doi: 10.1145/3308560.3316738.

[76] B. Wilder and Y. Vorobeychik, ‘‘Defending elections against malicious spread of misinformation,’’ in Proc. AAAI, vol. 33, Jul. 2019, pp. 2213– 2220, doi: 10.1609/aaai.v33i01.33012213.

[77] P. Nemitz, ‘‘Constitutional democracy and technology in the age of artificial intelligence,’’ Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci., vol. 376, no. 2133, Nov. 2018, Art. no. 20180089, doi: 10.1098/rsta.2018.0089.

[78] L. Floridi and M. Chiriatti, ‘‘GPT-3: Its nature, scope, limits, and consequences,’’ Minds Mach., vol. 30, pp. 681–694, Nov. 2020, doi: 10.1007/s11023-020-09548-1.

[79] K. McGuffie and A. Newhouse, ‘‘The radicalization risks of GPT-3 and advanced neural language models,’’ 2020, arXiv:2009.06807.

[80] Wordflow AI Articles. Accessed: Apr.

[81] R. Leyva and C. Beckett, ‘‘Testing and unpacking the effects of digital fake news: On presidential candidate evaluations and voter support,’’ AI Soc., vol. 35, no. 4, pp. 969–980, Dec. 2020, doi: 10.1007/s00146-02000980- 6

[82] S. M. Jones-Jang, T. Mortensen, and J. Liu, ‘‘Does media literacy help identification of fake news? Information literacy helps, but other literacies don’t,’’ Amer. Behav. Scientist, vol. 65, no. 2, pp. 371–388, Feb. 2021, doi: 10.1177/0002764219869406.

[83] Association for College and Research Libraries. (2016). Framework for Information Literacy for Higher Education. Accessed: Jun. 29, 2021. [Online]. Available: https://www-ala-org.proxyub.rug.nl/acrl/standards/ilframework

[84] O. J. Gstrein, ‘‘Right to be forgotten: European data imperialism, national privilege, or universal human right?’’ Rev. Eur. Administ. Law, vol. 13, no. 1, pp. 125–152, May 2020, doi: 10.7590/187479820X15881424928426.

[85] H. Allcott and M. Gentzkow, ‘‘Social media and fake news in the 2016 election,’’ J. Econ. Perspect., vol. 31, no. 2, pp. 211–236, May 2017, doi: 10.1257/jep.31.2.211.

[86] C. Shah. (Mar. 10, 2021). It’s Not Just a Social Media Problem—How Search Engines Spread Misinformation. The Conversation. Accessed: Jun. 29, 2021. [Online]. Available: http://theconversation.com/itsnotjust-a-social-media-problem-how-search-enginesspreadmisinformation-152155

[87] C. Arun, ‘‘Facebook’s faces,’’ in Forthcoming Harvard Law Review Forum, vol. 135. Mar. 2021, doi: 10.2139/ssrn.3805210.

[88] G. De Gregorio, ‘‘Democratising online content moderation: A constitutional framework,’’ Comput. Law Secur. Rev., vol. 36, Apr. 2020, Art. no. 105374, doi: 10.1016/j.clsr.2019.105374.

[89] R. T. Garcia. (Jun. 19, 2020). Anonymous Twitter Accounts in Brazil are Pressuring Advertisers to Drop Conservative Media Campaigns. Insider. Accessed: Jun. 29, 2021. [Online]. Available: https://www.insider.com/sleeping-giants-brasil-borrowing-us-tacticforfighting-misinformation-2020-6

[90] J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Niessner, ‘‘Face2Face: Real-time face capture and reenactment of RGB videos,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016, pp. 2387–2395.

[91] M. Westerlund, ‘‘The emergence of deepfake technology: A review,’’ Technol. Innov. Manage. Rev., vol. 9, no. 11, pp. 39–52, Jan. 2019, doi: 10.22215/timreview/1282.

[92] T. Greene. (Apr. 21, 2020). Watch: Fake Elon Musk Zoom-Bombs Meeting Using Real-Time Deepfake AI. Neural | The Next Web. Accessed: Apr. 7, 2021. [Online]. Available: https://thenextweb.com/ neural/2020/04/21/watch-fake-elon-musk-zoom-bombs-meetingusingreal-time-deepfake-ai/

[93] L. Guarnera, O. Giudice, C. Nastasi, and S. Battiato, ‘‘Preliminary forensics analysis of DeepFake images,’’ 2020, arXiv:2004.12626.

[94] M.-H. Maras and A. Alexandrou, ‘‘Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos,’’ Int. J. Evidence Proof, vol. 23, no. 3, pp. 255–

[95] D. O’Sullivan. (Aug. 10, 2019). The Democratic Party Deepfaked Its Own Chairman to Highlight 2020 Concerns. CNN. Accessed: May 11, 2020. [Online]. Available: https://www.cnn.com/2019/08/09/ tech/deepfake-tom-perez-dnc-defcon/index.html

[96] D. Fonseca. (Jan. 18, 2021). BrunoSartori:OReiDASDeepfakes. Revista Trip. Accessed: Jun. 28, 2021. [Online]. Available: https://revistatrip. uol.com.br/trip/webstories/bruno-sartori-o-rei-das-deepfakes

[97] J. Compton, ‘‘Inoculation theory,’’ in SAGE Handbook of Persuasion: Developments in Theory and Practice. Newbury Park, CA, USA: Sage, 2012, pp. 220–236, doi: 10.4135/9781452218410.n14.

[98] W. J. McGuire, ‘‘Inducing resistance to persuasion: Some contemporary approaches,’’ in Advances in Experimental Social Psychology, vol. 1, L. Berkowitz, Ed. New York, NY, USA: Academic, 1964, pp. 191–229.

[99] D. Guera and E. J. Delp, ‘‘Deepfake video detection using recurrent neural networks,’’ in Proc. 15th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), Auckland, New Zealand, Nov. 2018, pp. 1–6, doi: 10.1109/AVSS.2018.8639163.

[100] R. Chesney and D. K. Citron, ‘‘Deep fakes: A looming challenge for privacy, democracy, and national security,’’ SSRN J., pp. 1753–1820, 2018, doi: 10.2139/ssrn.3213954.

[101] V. Elliott and M. Tobin. (Jan. 10, 2022). China Steps up Efforts to Ban Deepfakes. Will it work? Rest World. Accessed: Mar. 1, 2022. [Online]. Available: https://restofworld.org/2022/china-steps-upeffortsto-ban-deepfakes/

[102] K. Zetter. (Nov. 19, 2010). Wiseguys Plead Guilty in Ticketmaster Captcha Case. Wired. Accessed: Jun. 2, 2020. [Online]. Available: https://www.wired.com/2010/11/wiseguys-plead-guilty/

[103] K. Trieu and Y. Yang. (2018). Artificial Intelligence-Based Password Brute Force Attacks. [Online]. Available: http://aisel.aisnet.org/ mwais2018/39

[104] D. Gibert, C. Mateu, and J. Planes, ‘‘The rise of machine learning for detection and classification of malware: Research developments, trends and challenges,’’ J. Netw. Comput. Appl., vol. 153, Mar. 2020, Art. no. 102526, doi: 10.1016/j.jnca.2019.102526.

[105] AV-TEST. (2021). Malware Statistics & Trends Report. AV-TEST: The Independ. IT-Security Inst. Accessed: Jun. 22, 2021. [Online]. Available: https://www.av-test.org/en/statistics/malware/

[106] (2018). DeepLocker—Concealing Targeted Attacks With AI Locksmithing. Black Hat USA. Accessed: Apr. 22, 2021. [Online]. Available:

https://www.blackhat.com/us18/briefings/schedule/#deeplocker— concealing-targeted-attacks-withai-locksmithing-11549262, Jul. 2019, doi: 10.1177/1365712718807226. [95] D. O'Sullivan. (Aug. 10, 2019). The Democratic Party Deepfaked Its Own Chairman to Highlight 2020 Concerns. CNN. Accessed: May 11, 2020. [Online]. Available: https://www.cnn.com/2019/08/09/ tech/deepfake-tom-perez-dnc-defcon/index.html [96] D. Fonseca. (Jan. 18, 2021). BrunoSartori:OReiDASDeepfakes. Revista Trip. Accessed: Jun. 28, 2021. [Online]. Available: https://revistatrip. uol.com.br/trip/webstories/bruno-sartori-o-rei-das-deepfakes