



## Article

# Avoidance of Cybersecurity Threats with the Deployment of a Web-based Blockchain-Enabled Cybersecurity Awareness Model

Abdul Razaque <sup>1,\*</sup>, Abrar Al Ajlan <sup>2</sup>, Noussaiba Melaoune <sup>3</sup>, Munif Alotaibi <sup>4</sup> , Bandar Alotaibi <sup>5,6</sup> , Issabekov Dias <sup>1</sup>, Ammar Oad <sup>7</sup>, Salim Hariri <sup>8</sup>, Zhao Chenglin <sup>7</sup>

- <sup>1</sup> Department of Information Security, International Information Technology University, Almaty Kazakhstan
- <sup>2</sup> Self-Development Skills Department, Common First Year Deanship, King Saud University, Saudi Arabia
- <sup>3</sup> Department of Computer Science and Information Technology, University Mohammed V Rabat, Morocco
- <sup>4</sup> Department of Computer Science, Shaqra University, Shaqra, 15526, Saudi Arabia
- <sup>5</sup> Department of Information Technology, University of Tabuk, Tabuk, 47731 Saudi Arabia; b-alotaibi@ut.edu.sa
- <sup>6</sup> Sensor Networks and Cellular Systems (SNCS) Research Center, University of Tabuk, Tabuk, 47731, Saudi Arabia
- <sup>7</sup> Faculty of Information Engineering, Shaoyang University, Shaoyang, China
- <sup>8</sup> Department of Electronics and Computer Engineering, University of Arizona, USA
- \* Correspondence: a.razaque@iitu.kz

**Abstract:** The ignorance of or lack of knowledge about cybersecurity aspects causes a critical problem regarding confidentiality and privacy. This security problem will continue to exist even if the user possesses less expertise in information security. The modern IT technologies are well developed, and almost everyone uses the features of IT technologies and services within the Internet. However, people are being affected due to cybersecurity threats. People can adhere to the recommended cybersecurity guidelines, rules, adopted standards, and cybercrime preventive measures. However, it is not possible to entirely avoid cybercrimes. Cybercrimes often lead to sufficient business losses and spread forbidden themes (hatred, terrorism, child porn, etc.). Therefore, to reduce the risk of cybercrimes, a web-based Blockchain-enabled cybersecurity awareness program (WBCA) process is introduced in this paper. The proposed web-based cybersecurity awareness program trains users to improve their security skills. The proposed program helps with understanding the common behaviors of cybercriminals and improves user knowledge of cybersecurity hygiene, best cybersecurity practices, modern cybersecurity vulnerabilities, and trends. Furthermore, the proposed WBCA uses the Blockchain technology to protect the model from the potential threats. The proposed model is validated and tested using real-world cybersecurity topics with real users and cybersecurity experts. We anticipate that the proposed program can be extended to other domains, such as national or corporate courses, to increase the cybersecurity awareness level of users.



**Citation:** Abdul Razaque; Abrar Al Ajlan; Noussaiba Melaoune; Munif Alotaibi; Bandar Alotaibi; Issabekov Dias; Ammar Oad; Salim Hariri; Zhao Chenglin Avoidance of Cybersecurity Threats with the Deployment of a Web-based Blockchain-Enabled Cybersecurity Awareness Model. *Preprints* 2021, 11, 0. <https://doi.org/>

Received:

Accepted:

Published:

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Keywords:** Information security; Cybercrime; cyber awareness; cybersecurity basics; cybersecurity hygiene; Blockchain technology

## 1. Introduction

Currently, the main trending problem concerns issues regarding cybersecurity aspects, especially the knowledge of information security basics. Information security is a concept is becoming increasingly enmeshed in many aspects of our society, largely as a result of our nearly ubiquitous adoption of computing technology [1]. Cybersecurity consists of largely defensive methods used to detect and thwart would-be intruders [2]. The majority of people have tunnel vision regarding information security basics, and they do not know much about other ways to consider and improve cybersecurity awareness. Despite the level of spending, public awareness, and preparedness in certain fields, most users do not yet think of computer security as anything but a nuisance [3]. Cybercrime will more than triple the number of job openings over the next 5 years [4]. Cybercrime can be regarded as computer-mediated activities that are either illegal or considered illicit by certain parties, and they can be conducted through global electronic networks [5].

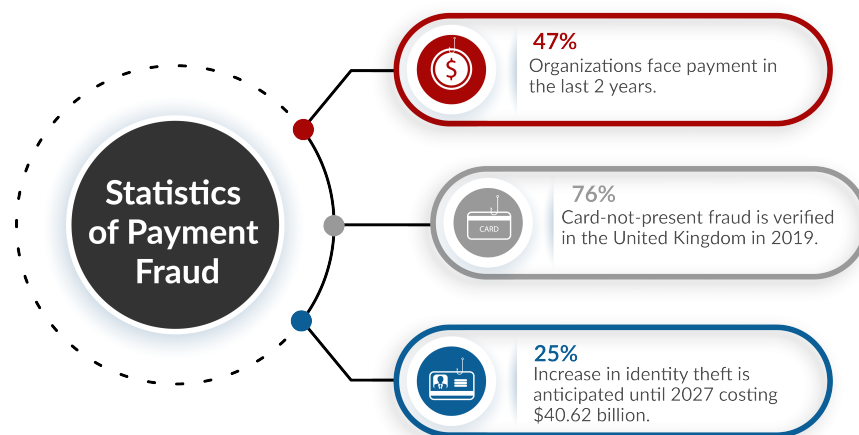
Therefore, the main question “Is it possible to avoid any cybercrime by knowing the basics of cybersecurity?” remains in the mainstream. Since modern technologies are used everywhere globally and by almost everyone on the Internet, this issue affects all of them. Cybercrime is switching its battleground from desktops to other platforms, including mobile phones, tablet computers, and VoIPs [6]. It includes stealing, such as by capturing everything people type, including passwords, credit card numbers, and bank account numbers [7]. Cyber fraud, stealing, phishing, and other malicious behaviors will enrich the terminology of cybercrime in the years ahead [8]. It is not sufficient to only follow the recommended cybersecurity standards, rules, and anti-cybercrime actions to avoid cybercrimes. Therefore, there are obvious risks caused by this problem, such as large business losses and the spreading of forbidden themes, such as racial/national/global hate, terrorism, cyberterrorism, and child porn.

Cybercrime emerged in the late 1970s as the computer information technology (IT) industry took shape [9]. Security is being employed now and it is in the news – it is alive and kicking [10].

As an increasing number of users and businesses use technologies, cybersecurity and its awareness are becoming the most predominant issues. Some cybercriminals are motivated by financial gain, whereas others seek to obtain intellectual property or consumer information, to damage an institution’s reputation, or to make a political statement through “hacktivism” [11]. People should spend less in anticipation of cybercrime (on antivirus programs, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail [12]. The main problems are to determine the common mistakes in the behaviors of people based on their current cybersecurity knowledge and provide recommendations for protecting against cybercrimes so that businesses can be more resistant to cybersecurity attacks.

Even if law enforcement reduces the rate of cybercrimes, the issue is not about how to avoid them technically [13]. The lack of organizational stability and continuity in the field of cybercrime policing may itself disrupt efforts to effectively tackle the problem of online crime [14].

To realize cybersecurity awareness, the following should be considered: (a) determine the various security topics and programs available for cybersecurity training, (b) investigate common mistakes in human behavior, and (c) determine the methods by which cybercriminals act. We are working to address these problems and use these solutions in life to protect people from cybercrimes. For instance, a user can set the Microsoft Internet Explorer browser with a predefined security level (Low, Medium Low, Medium, or High). As shown in figure 1, it is anticipated by [15] that an increase of 25% in identity theft until 2027 costing \$40.62 billion. Considerable effort is made each year by the government and private sector organizations in seeking to educate consumers regarding the risks of identity crime, especially the forms that occur online [16,17]. Another way to avoid cybercrime is to protect people from cybercriminals with the advantages of existing laws [18]. However, this disintermediation of the news process runs counter to the construction of the imagery surrounding cybercrime, which originated in the days before the Internet when the mass media was organized more centrally [19].



**Figure 1.** Statistics of payment fraud.

## 2. Research Problem

The very extensive and difficult problem at hand is a lack of knowledge regarding information security basics, and its significance will become increasingly relevant as new technologies are developed. For instance, in the future, people will use modern technologies, and in parallel, the need for full protection of these technologies will grow. All global businesses, including large corporations and companies, will bring innovations to life. However, this is insufficient. Moreover, if the world needs good specialists for the development of these technologies (and there are very few), there will be an even greater need for cybersecurity specialists (especially those who protect the masses in such ways).

### 2.1. Research Importance

It is very important not only to know the basics of cybersecurity but also to see the whole picture of cybercrime so as not to become another victim of cybercriminals. The point is that most types of cybercrime require an organization with execution as well as profitability [20]. In other words, knowledge is light, and ignorance is darkness. This problem also concerns information security. The varying attack types in existence illustrate how it is difficult to put any single exact, meaningful label on the size of the problem [21].

### 2.2. Possible Research Solutions

To reduce the risk of cybercrimes, the possible solutions to this problem are as follows:

- The study of common mistakes individuals makes, which lead to being the victims of cybercriminals, and taking advantage of these experiences;
- The development of a web-based program that will test for the common behaviors of cybercriminals;
- Monitoring the impact of cybercrime and giving a new view of cybercrimes by using the advantages of much cybersecurity information;
- The creation of more cybersecurity seminars and training programs about the cyber-crime world and cybersecurity hygiene;
- The analysis and usage of advice from cybersecurity professionals and modern cybersecurity trends to prevent cybercrimes

However, the most feasible solution from an efficiency perspective is to train users with the developed web-based program, which tests their cyber awareness levels. This should be implemented as a Linux-based web server, which holds a program that determines the cybersecurity awareness of the users. Additionally, there should be deployed Blockchain technology to protect the model from potential threats.

### 2.3. Research Contribution

The contributions of this work, which are motivated by the above challenges, are summarized as follows:

- The developed web-based program helps many people test and improve their cybersecurity awareness levels
- The developed web-based program is guaranteed to determine the cybersecurity bottlenecks of the tested users.
- Determining the level of cybersecurity knowledge possessed by the tested users enables the program to use the collected data to evaluate the cybersecurity bottlenecks and the appropriate mitigation methods for minimizing the risk of being victimized by cybercriminals.
- The program results can be analyzed to train the tested users on advanced cybersecurity topics to preserve high cybersecurity awareness among them.
- The Blockchain technology is used to protect WBCA model from any potential malicious threats.

### 2.4. Research Structure

The remainder of the paper is organized as follows. Section 3 presents the features of the existing literature. Section 4 presents the state-of-the-art system model. Section 5 presents the proposed cybersecurity awareness process. Section 6 presents the experimental results and provides the discussion of the results. Finally, the conclusions of the paper are presented in Section 7.

## 3. Related Work

In this section, the main characteristics of current approaches are deliberately discussed. Today, people utilize several cybersecurity approaches to make themselves more secure. One of the effective cybercrime mitigation approaches is the Point-of-sale device [22]. It offers protection from malicious codes that track online activities and may capture everything they type, including passwords, credit card numbers, and bank account numbers. This type of software is one of the best solutions because it protects the computer and data from being automatically stolen by malicious software. However, it can be used only locally on personal computers, and the software often requires payment for use.

In addition, the “law enforcement strike back” was introduced in [23]. This principle suggests that countries let law enforcement officers use ‘electronic sanctions’ to react to cybercrime, including the dissemination of viruses, worms, and other types of malware, along with hacking and denial-of-service attacks. Indeed, law enforcement reduces the rate of cybercrimes. However, the law authors are limited to general information security, and this approach does not cover specific topics and steps to technically avoid cybercrimes.

In addition, web browser-based protection from malicious code is an effective suggestion [24]. Therefore, this solution is to set the desired browser security level. For example, malicious JavaScript, Java, and ActiveX code can be blocked; the Microsoft Internet Explorer web browser allows the selection of a predefined security level (Low, Medium Low, Medium, or High). Finally, monitoring and protection can be designed to identify almost every malicious web attack. However, such a technique does not explain how it identifies these attacks and does not protect browsers from zero-day attacks.

The focus on scaling the varying attack types was proposed by the authors in [21]. The main idea is to widen the scale of problems related to cybercrimes and the community. However, the authors did not consider the difficult problems caused by scaling these issues. According to the cybersecurity protection problem, the development of user education and victim support was introduced in [25]. That is, if suspicious actions are observed for a given account, the technical staff must delete the malicious phishing information. However, this support does not properly cover the scale of the overall victim rate.

Additionally, a method for reducing the risk of being victimized by cybercrime is to use businesses’ countermeasures to combat cybercrimes [26]. In addition to preventive

rules, there are also corporate-level rules to prevent cybercrimes. However, it may not be sufficient to enforce only these business countermeasures; this method requires a worldwide scale as well.

The main aspects of cybercrime existence are organization and profitability, as explained by the authors in [27]. The authors suggested focusing on these factors to successfully avoid cybercrimes. However, other possible factors that drive cybercriminals were not considered.

Finally, another method for mitigating cybercrime is to stick to the cybersecurity NIST [20]. It is a cybersecurity framework that provides a performance-based and cost-effective approach to help organizations identify, assess, and manage cybersecurity risks. The NIST perceives that as information security and technology innovation advance, people must continue adjusting to configurations, and fundamental online protection practices must be created, actualized, maintained, and persistently improved. It is a good framework for deploying cybersecurity management schemes and regulations to plan against cybercrime incidents. However, this framework does not cover the idea of the technical avoidance of cyber-threats. In this paper, we introduce a new web-based program for a practical implementation that tests the cybersecurity awareness levels of users, where they are tested on basic and advanced cybersecurity topics; this approach will then minimize the risks of being a victim of cybercriminals. Another decision made was to reduce “hacktivism”. Some cybercriminals are motivated by financial gain, whereas others seek to obtain intellectual property or consumer information, damage an institution’s reputation, or make a political statement through “hacktivism” [11]. However, the authors did not consider other local aspects.

A previously proposed solution was to analyze the development of cybercrime. Cybercrime will more than triple the number of job openings over the next 5 years [28]. It is good to collect data to effectively prevent similar situations in the future. However, the authors could not cover all data.

The detection of cybersecurity threats was another previously proposed solution based on deep learning [29]. Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders. Defensive methods are necessary for information security. However, the authors did not mention the special tools used to do so.

Making people more aware of various malicious behaviors is of high importance. Cyber fraud, stealing, phishing, and other malicious behaviors will enrich the terminology of cybercrime in the years ahead [30]. However, these authors did not include all malicious actions.

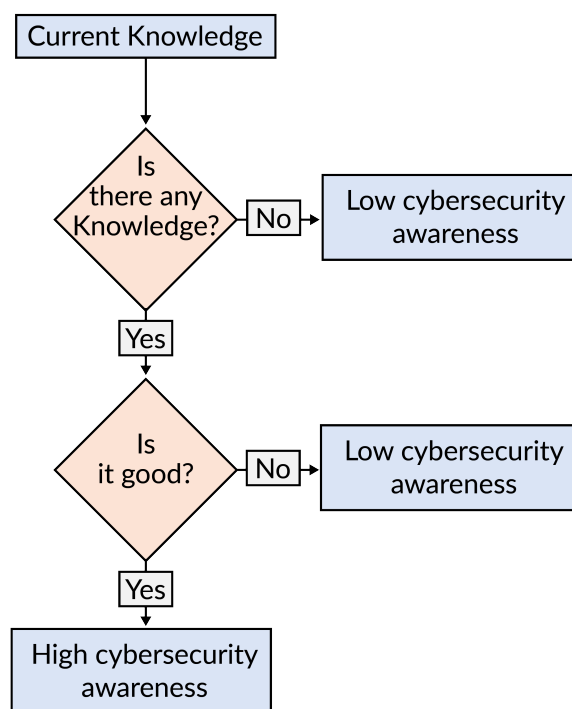
#### 4. System Model

This section presents a system scenario for calculating the information security awareness of users on the Internet and in network spaces. First, before we define the system model’s components, we should know that cybercrime is a crime committed on the Internet, on networks, or even against stationary computers. The cybersecurity awareness web program is significant software among the growing information security trends. To prove the limitations of the lack of cybersecurity basics, the system model consists of four parts:

- An initial knowledge-check
- A lower cybersecurity awareness module
- An advanced knowledge check
- A high cybersecurity awareness module

The initial knowledge check module checks the information security basics known by the user. The lower cybersecurity awareness module is responsible for identifying the low awareness of the user and giving appropriate feedback for the user’s bottlenecks. The advanced knowledge check module assesses the advanced information security basics possessed by the user. The high cybersecurity awareness module also identifies the high awareness of the user and gives appropriate feedback for the current user’s bottlenecks.

These four parts work consecutively through logical examinations and result retrievals, as shown through the blocks and arrows in the dataflow diagram depicted in Figure 2. First, it is necessary to ensure that the user has good knowledge of information security, and the program initially checks the current knowledge. If the user does not have this knowledge, then the situation is classified as “poor awareness” and the result is provided as “low cybersecurity awareness”. The next step is to check if the tested user has good knowledge. If the result is positive, the aggregation concludes that the user has excellent information security awareness (high cybersecurity awareness). Therefore, using this system model, we can determine the user’s cybersecurity awareness level. The system model realizes the need for increasing the cybersecurity awareness of users. If this model is implemented in the real world, the risks of cybercrimes can be minimized as users become more aware of information security basics. The use of a cybersecurity awareness web program not only ensures a high cybersecurity awareness level while testing users but also improves cybersecurity training efficiency.



**Figure 2.** The process of defining the cybersecurity awareness of the user.

## 5. Proposed Blockchain-enabled Cybersecurity Awareness Process

This section shows the mechanism of how user knowledge is calculated in the field of information security in detail. The proposed WBCA consists of following processes.

- Counter Sorting Process
- Cybersecurity Awareness Assessment Process
- Blockchain-Enabled Susceptibility Detection Process

### 5.1. Counter Sorting Process

The proposed main components are used to calculate accurate results from the user’s replies, sort them and arrange them so that the efficiency for each topic can be viewed. Each step defines the degree of aptitude that the user shows during testing on the web server. For this algorithm, we used the counting sort algorithm as a baseline sorting method to check the input entries of each user to assess their knowledge of cybersecurity. The counter sort approach is an efficient process for sorting an array of elements, each with a nonnegative integer key mapped to the elements by some alphabet-to-numeric conversion



scheme. It is a stable sorting technique that is used to sort objects according to keys that are small numbers. It counts the number of keys whose key values match. This sorting method is effective when the difference between different keys is not large; otherwise, it can increase the complexity of the space. Thus, its time complexity is given by:

$$T_c = O(n + r) \quad (1)$$

where  $T_c$  is the time complexity;  $O(n + r)$  is the time function for measuring performance;  $n$  is the number of elements and  $r$  is an element's degree.

At the same time, its spatial complexity is identical:

$$S_c = O(n + r) \quad (2)$$

where  $S_c$  is the space complexity.

The sorting process maps  $M$  the following input/output pairs:

$$M_{(I)} = \sum_{i=0}^{n-1} i \{A_{[0]} + A_{[n+1]} + \dots + A_{[n-1]}\} \quad (3)$$

where  $A$  is an array to be summed, and  $M_{(I)}$  is the input mapping.

The process outputs a sorted permutation of  $A$ , called  $B$ , such that:

$$M_{(O)} = \sum_{i=0}^{n+1} i \{B_{[0]} + B_{[n-1]} + \dots + B_{[n+1]}\} \quad (4)$$

where  $B$  is a sorted permutation of array  $A$ , and  $M_{(O)}$  is the output mapping.

## 5.2. Cybersecurity Awareness Assessment Process

It comprises of a function with variables, and the function itself is based on the checking process for defining cybersecurity awareness. The function gives a positive output if and only if the following condition is true: The current cybersecurity knowledge is related to the good knowledge given by

$$F(x) = \forall x(x \in G_k \wedge x \notin B_k) \quad (5)$$

where  $x$  is the current cybersecurity knowledge;  $G_k$  is the good cybersecurity knowledge; and  $B_k$  is the bad cybersecurity knowledge.

In algorithm 1, the process of defining cybersecurity awareness is shown.

---

### Algorithm 1 Cybersecurity awareness assessment process

---

**Input:**  $C_K, B_K, G_k$  in

**Output:**  $G_k$  or  $B_K$  out

- 1: **Initialization:**  $\{C_K$ : Current knowledge;  $B_K$ : Bad knowledge;  $G_k$ : Good knowledge ;  $A_l$ : Low cybersecurity awareness;  $A_h$ : High cybersecurity awareness;
  - 2: **Check**  $C_K \in B_K$
  - 3: **if**  $C_K \in B_K$  **then**
  - 4:     **Show**  $A_l$
  - 5:     **Check**  $C_K \in G_k$
  - 6: **end if**
  - 7: **if**  $C_K \in G_k$  **then**
  - 8:     **Show**  $A_h$
  - 9: **end if**
  - 10: **if**  $C_K \notin B_K$  and  $C_K \notin G_k$  **then**
  - 11:     **Show**  $A_l$
  - 12: **end if**
-

In algorithm 1, the cybersecurity awareness definition process is explained. In step 1, the variables are initialized to determine the process. At the beginning of the algorithm, the input and output processes are given to evaluating cybersecurity knowledge, respectively. Step 2 makes an initial check to see if the current cybersecurity knowledge is bad. Consequently, in step 4, the program shows the result as low knowledge. Next, steps 5-7 check if the current cybersecurity knowledge is good. Therefore, in steps 8-10, if the current cybersecurity knowledge is good, then the program outputs "high knowledge". Finally, in step 11, the program determines whether the current information security basics are defined as neither good nor bad; it generally outputs this result as low knowledge by default. Using the results, it can be concluded that if the program outputs bad knowledge, it shows that the tested user has low cybersecurity awareness. Otherwise, the user has high cybersecurity awareness.

Let us define the cybercrime rate  $C_r$  of the user that can be calculated as it relates to current knowledge:

$$C_r = C_k \times 100\% \quad (6)$$

Next, the overall cybercrime risk is used to assess the user's risk of being the victim of a cybercrime, which can be calculated by:

$$R_c = \frac{C_r + G_k}{B_k} \quad (7)$$

where  $R_c$  is the overall cybercrime risk of the user.

On the other hand, the cybercrime delta between good cybersecurity knowledge and bad cybersecurity knowledge is shown in the following equation:

$$C_d = \frac{1}{G_k - B_k} \quad (8)$$

To calculate the inverse proportion of equation 6, which is necessary to find the correct current knowledge, the equation is:

$$\text{However, } C_k = \frac{C_r}{100\%} \quad (9)$$

Consequently, equation 9 is simplified in this way, which is helpful for using only the current knowledge dependency:

$$R_c = \frac{C_k(G_k + 1)}{B_k \times 100\%} \quad (10)$$

Based on the essential steps explained in the algorithm 2, it is necessary to use the modulus of the cybersecurity awareness level. Therefore, the formula is as follows:

$$S_r = G_k \times 100\% \quad (11)$$

where  $S_r$  denotes a successful result of the program's test.

In other words, if the results are positive, then the user has high cybersecurity awareness:

$$F(S_r) = \forall x((x \in G_k) \wedge (x \in S_r)) \quad (12)$$

**Theorem 1.** Suppose first that the user obtains good results from a web-based program. Consequently, the user has a good cybersecurity awareness  $G_k$ . Therefore, if the user has high cybersecurity awareness, then the risk of being the victim of cybercrimes is low  $R_l$ .

**Proof.** First, let us define the second instance of the theorem; thus, the following formula defines the high cybersecurity awareness as being inversely proportional to the risk of being a victim:  $\square$



$$G_k = \frac{1}{R_l} \quad (13)$$

Consequently, we have two separate instances as follows. This is helpful for defining the bounds of the estimated program results:

$$(G_k + S_r)^u = \sum_{k=0}^n \binom{k}{u} \left(\frac{1}{R_l}\right)^k G_k^{u-k} \quad (14)$$

where  $u$  is the upper bound and  $k$  is the lower bound. Now let us use the relative formula of good results and the sine equation for the first and second instances, which in turn should be used to check further graph data:

$$S_r = \frac{1}{R_l} \times \pi \quad (15)$$

$$\sin(S_r) = 2\pi \times \sin\frac{1}{2}(R_l) \quad (16)$$

As a result, equation 15 squared together with the first instance is inversely proportional to low cybercrime risk ( $\pi$  is constant and removed from the formula), and the following equation is helpful for estimating the program results twice:

$$S_r^2 = \frac{1}{R_l^2} \quad (17)$$

Consequently, combining the equations of  $S_r$  and the sine of  $S_r$  make the sine-based view of the estimated results more accurate:

$$\sin\left(\frac{1}{R_l} \times \pi\right) = 2\pi \times \sin\frac{1}{2}(R_l) \quad (18)$$

Therefore, it is mathematically proven that if the user has good program results, then the risk of being the victim of cybercrimes is lower.

**Corollary 1.** *If the user has bad results from the web-based program, then their risk of being the victim of cybercrimes is high.*

*Good cybersecurity basics are now substituted by poor cybersecurity basics. Therefore, we have the corresponding cosine version of the equation:*

$$\cos\left(\frac{1}{R_l} \times \pi\right) = 2\pi \times \cos\frac{1}{2}(R_l) \quad (19)$$

**Theorem 2.** *If the user has high cybersecurity awareness  $H_s$ , then the user has a low chance of being the victim of cybercrimes  $L_c$ . However, the user has a high chance of being a victim of cybercrimes. Therefore, the user's cybersecurity awareness is low.*

**Proof.** First, the given instances of this theorem are shown below, which demonstrate that if there is any current knowledge, it belongs to the high awareness category:  $\square$

$$F(L_c) = \forall C_k (C_k \in H_s) \quad (20)$$

where  $H_s$  is the user's high cybersecurity awareness and  $L_c$  denotes a low chance of being the victim of cybercrimes.

Next, assuming that the user has high cybersecurity awareness, let us integrate this assumption with equation (20):

$$\int_0^{L_c} H_s^2 dH_s = \frac{L_c^3}{3} \quad (21)$$

Now let us use the conjunction of equation 15 with the negation of,  $H_s$ , which describes an integral part of high awareness between low chances and ordinary chances:

$$A(H_s) = \int_c^{L_c} (H_s) dH_s \quad (22)$$

Next, let us define the mean of the low risk and low chance situations through the integration of the function of  $H_s$ :

$$A(H_s) = \int_0^{R_l+L_c} f(H_s) dH_s = \frac{(R_l + L_c)^2}{2} \quad (23)$$

Finally, the conditional equations of the negation of  $H_s$  and its cosine function are obtained, so we have the functional result of the integral parts:

$$f(H_s) = \frac{A(H_s + L_c) - A(x)}{x} \quad (24)$$

As a result, the user has a high chance of being the victim of cybercrimes, and the user has low cybersecurity awareness. The theorem is proven.

**Property 1.** *Cyber awareness Nondualism – the cyber awareness score result is always a positive or negative number.*

For instance, if the final score of the web program shows bad cybersecurity knowledge, the output is a negative number. Otherwise, the program gives a positive number instead.

$$F(R_p) = \exists x((x \in G_k) \wedge (x \in B_k)) \quad (25)$$

where  $R_p$  is the web program result

In conclusion, we observe that the results of the proposed WBCA deduce only two results: good cybersecurity knowledge or bad cybersecurity knowledge.

### 5.3. Blockchain-Enabled Susceptibility Detection Process

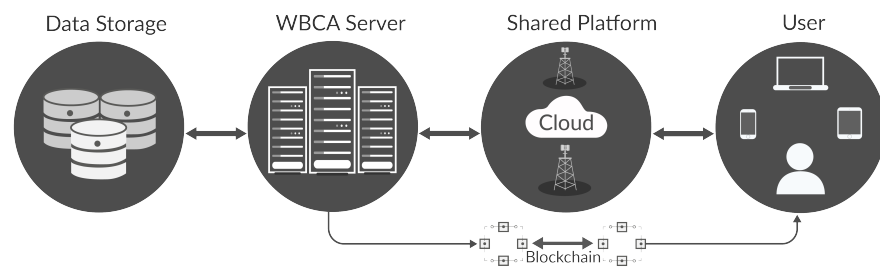
The Blockchain activates the distributed ledger by replacing the existing centralized ledger structure. It provides security using hash encryption and public key cryptographic algorithm. Our proposed WBCA is deployed on the cloud. Therefore, it is the possibility to be exposed the vulnerability of the cloud and launched threats on the WBCA server by the attacker. The attacker can generate similar cybersecurity tasks using the same digital signature because double occurrence is possible. The attacker can make it realty if it has a robust hashing capability and generated a longer private chain as compared to public-key cryptography to perform such events. The probability of the susceptibility detection  $P_{sd}$  is given by:

$$P_{sd} = \left(\frac{x}{y}, 1\right)^{\max(y+1, 0)} \begin{cases} 1 & \text{if } \gamma < 0, x > y \\ \left(\frac{x}{y}\right)^{y+1} & \text{if } \gamma \geq 0, x \leq y \end{cases}$$

where  $x, y$  are hash parameters of the legitimate user and attacker respectively.  $\gamma$  is the number of the blocks used by the WBCA model that provides an edge over the attacker.

If  $\gamma$  turns into positive, then the proposed WBCA model is capable of sending the blocks and overtake the illegitimate users. The Blockchain-enabled susceptibility detection model for WBCA is shown in Figure 3. The WBCA server can transmit the data using

Blockchain-enabled technology to restrict the potential threats encountered by the attacker. The Blockchain susceptibility detection process is explained in algorithm 2.



**Figure 3.** Blockchain-Enabled susceptibility detection model for WBCA.

**Algorithm 2** Blockchain susceptibility detection Process of defining the user's vulnerability

**Input:**  $C_U, I_U, R_U$  in

**Output:**  $C_p$  or  $C_r$  out

- 1: **Initialization:**  $\{C_U$ : Current user;  $C_p$ : Cybercrime prone;  $C_r$ : Cybercrime resistant;  $I_U$ : Insecure user;  $R_U$ : Reliable user; $\}$
- 2: **Check**  $C_U \in I_U$
- 3: **if**  $C_U \in I_U$  **then**
- 4:   **Show**  $C_p$
- 5: **end if**
- 6: **if**  $C_U \in R_U$  **then**
- 7:   **Show**  $C_r$
- 8: **end if**
- 9: **if**  $C_U \notin R_U$  **then**
- 10:   **Show**  $C_p$
- 11: **end if**

Algorithm 2 shows the process of defining the user's cybercrime proneness. In step 1, the variables are initialized to determine the process. The input and output processes are given at the beginning of the algorithm, respectively. Steps 2-3 check if the current user is insecure or reliable. If he/she is insecure, then in steps 4-5, the program outputs that the user is cybercrime prone. Next, step 6 checks if the user is reliable, then in steps 7-8, the web program outputs that the user is cybercrime resistant. Finally, in steps 10-11, if the current user is defined neither as insecure nor reliable, the program outputs the result as an insecure user by default.

**Corollary 2.** *If the user has a high chance of being a victim of attacker, then the user has low cybersecurity protection measures. The given chances tend to the maximum. Therefore, the cybersecurity protection is low.*

Now, we have an integral function to assess the integral of low chances between high chances and ordinary chances:

$$B(L_s) = \int_c^{H_c} L_s dL_s \quad (26)$$

where  $H_c$  is a high chance of being a cybercrime victim and  $L_s$  represents low cybersecurity awareness. Hence, the conditional function is the same as for the conditional equation, which again shows the functional result of the integral parts:

$$f(L_s) = \frac{B(L_s + H_c) - B(x)}{x} \quad (27)$$

**Property 2.** *Cyber awareness Nonidealism— the user's cybersecurity threat detection capability level always tends toward an idealistic result but never reaches it. For example, suppose that the user has 100% cybersecurity threat detection capability. However, as cutting-edge technologies are developed, the person must always observe the new cybersecurity trends.*

$$F(C_{td}) = \nexists x(x \in (C_a \times 100\%)) \quad (28)$$

where  $C_{td}$  is the cybersecurity threat detection capability level.

Based on the properties: 1-2, a hypothesis is introduced.

**Hypothesis 1.** *If  $C_{td} + R_p = S$ , where  $S$  is the overall security level;  $x, y$ , and  $z$  are natural numbers; and  $x, y$ , and  $z > 2$ ; then  $C_{td}, R_p$ , and  $S$  possess the common security criteria.*

**Proof.** To prove the hypothesis, let us introduce the entropy dependency of the input variables:

$$H(S^z) = H(C_a^x) + H(R_p^y) \quad (29)$$

where  $H(S^z)$  is the entropy of the security level;  $H(C_a^x)$  is the entropy of the cybersecurity threat detection capability level; and  $H(R_p^y)$  is the entropy of the web program result.  $\square$

This equation helps us obtain the hypothetical entropy results of the given variables.

As  $H(S)$  is the logarithm of  $S$  and other entropies are the logarithms of their variables, equation 29 gives the logarithmic form of these entropies:

$$\log_2 S^z = \log_2 C_a^x + \log_2 R_p^y \quad (30)$$

Now let us write the same equation in a shorter form:

$$\log_2 S^z = \log_2 C_a^x \times R_p^y \quad (31)$$

This gives the simplified form of equation 31. Consequently, let us simplify the equation; we see that using this simplest form, the overall security level consists of two factors: the cybersecurity threat detection capability level and the program results given by

$$S^z = C_a^x \times R_p^y \quad (32)$$

Next, we have system that gives the two dependency forms of the overall security level. From these systems, providing that  $x, y$ , and  $z > 2$ , we have a trivial solution, and the system  $S^z$  has only a single state:

$$\begin{cases} S^z = C_a^x \times R_p^y \\ S^z = C_a^x + R_p^y \end{cases} \quad (33)$$

Now let us introduce the common security criteria for the calculations to define the mean factor of the cybercrime rate of Blockchain-enabled susceptibility given by:

$$D = C_a^x \times R_p^y + S^z \quad (34)$$

where  $D$  denotes the common security criteria.

In addition to system 34, this formula achieves the summary of the overall security level plus its two independent factors.

Therefore, the common security criterion of  $S^z$  is  $D_{S^z} = D_{C_a^x} + 1$ , i.e., the criteria coefficients of  $C_a^x, S^z$  also differ by 1:

$$\begin{cases} R_p^y \times D_{S^z} = S^z \\ R_p^y \times D_{C_a^x} = C_a^x \end{cases} \quad (35)$$

where  $D_{S^z}^y$  denotes the common security criteria of  $S^z$  and  $D_{C_a}^y$  represents the common security criteria of  $C_a^x$ .

Now, we have proven the hypothesis, as this system finally shows that for each set of  $C_a$ ,  $R_p$ , and  $S$ , the common security criteria of Blockchain technology is achieved.

**Corollary 3.** For  $D = 0$ , the above equation has several solutions.

For example, as they are natural numbers, the various solutions can be shown in the following equation:

$$D_{C_a}^y = a_1((D_{S^z} + 1)^y - R_p^y) + 1 \quad (36)$$

That is, for  $D = 0$ , the equation indeed derives various solutions from the cybersecurity criterion for each set of  $C_a$ ,  $R_p$ , and  $S$ , so they have common security criteria.

**Property 3.** *Cyber awareness integrity – The user's overall security level consists of the user's susceptibility detection level and the positive or negative results obtained from the Blockchain technology. This property can be written as:*

$$D_{C_a}^y = a_1((D_{S^z} + 1)^y - R_p^y) + 1 \quad (37)$$

Therefore, the overall security level is the sum of the cybersecurity susceptibility detection level and the performance of the proposed WBCA model.

## 6. Experimental Results

This section demonstrates the experimental results regarding the experimental setup, performance metrics, and finally result discussion.

### 6.1. Experimental Setup

The proposed WBCA uses a web server installed on a CentOS-based Linux distribution. To achieve the stated goals, a CentOS-based virtual private server is deployed and tested in Almaty, Kazakhstan, where the model consistency, quality ratio, user response time, solution efficiency and threat avoidance capacity are monitored and calculated during testing process. The proposed WBCA is compared with the existing the state-of-the-art methods: Framework competence development and assessment(FCDA) [31], Integration of self-determination and flow (ISF) [32], modified total interpretive structural model (M-TISM) [33], Cybersecurity knowledge and skills(CKS) [34], and Cyber security awareness (CSA) [35].

These data are also calculated for the three most popular cybersecurity threats (email phishing, weak passwords, and virus). The minimal characteristics for the server hardware are Linux CentOS 7 x64 as the operating system, an Intel(R) Core (TM) i3-6100H with a frequency of 2.3 GHz and a cache size of 8192 kilobytes as the two-core processor, 4096 MB of random access memory, and a minimum of 50 gigabytes of hard disk space for collecting data. The required program component is Java SDK version 1.8.271u, and a monitor with a screen resolution of at least 920x1080 is used to conduct the proper experiments. These necessary characteristics for the web server are summarized in Table 1.

**Table 1.** Components of the web server.

Components	Version/The name of the system
Personal computer	x64
Operating system	Linux CentOS 7
Java version	1.8.271u
Recommended screen resolution	1920x1080
Processor	Intel(R) Core (TM) i3-6100H
Maker	Intel Xeon
RAM	4096 MB
Video memory	16 MB
Hard drive	50 GB (/dev/sda1)
CPU	2.300 GHz
Cache size	8192 KB

### 6.2. Performance Metrics

We determine the performance of the proposed WBCA and compared with the state-of-the-art contending models. Therefore, the following parameters are used for conducting the experiments:

- Consistency
- Quality Ratio
- User Response Time
- Solution Efficiency
- Threat Avoidance Capacity

#### 6.2.1. Consistency

The model consistency refers to the guarantee that the model follows the required rules to provide the stable outcomes. The user's basic cybersecurity awareness consistency is calculated using the following equation:

$$C = \frac{C_a}{T_a} \times 100\% \quad (38)$$

where  $C$  is the cybersecurity awareness consistency;  $C_a$  is the number of correct answers; and  $T_a$  is the total number of answers.

The data in Figure 4 demonstrate the correlation between the number of answered questions using the proposed WBCA and its comparison with other models. The result demonstrates the consistency and versus the time users take to solve the test questions. The calculated data used to define the cybersecurity awareness consistency levels of the tested users are depicted in Figure 4a, which illustrates the best cybersecurity topic (with 85% knowledge) demonstrates that our proposed WBCA produces 99.76% consistency; whereas the contending models show 97.4%-98.75% consistency. The CKS yields 97.4% consistency that is less than other contending models.

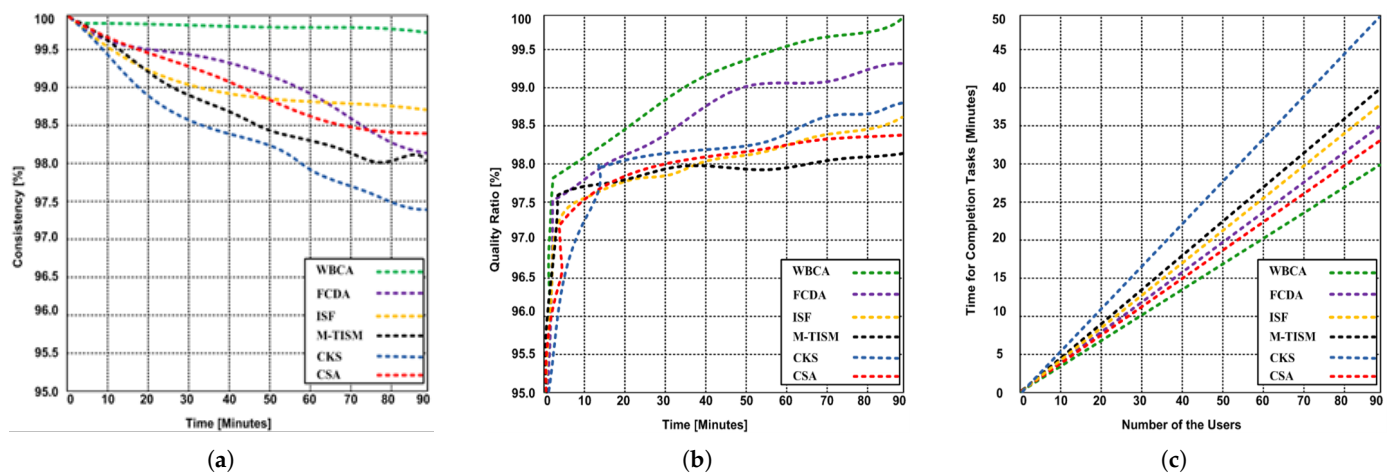
#### 6.2.2. Quality Ratio

It refers to a quantitative factor that controls how efficiently the model uses its parameters to produce high performance. The users who pass the tests on the basic cybersecurity topics are further tested on advanced cybersecurity themes. However, in these calculations, we use the following equation of the quality ratio:

$$Q = \frac{N_t}{T} \times 100\% \quad (39)$$

where  $Q$  is the quality ratio;  $N_t$  is the total number of steps used to solve advanced tasks; and  $T$  is the total time required to solve these tasks.





**Figure 4.** (a) Cybersecurity topic consistency using proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS). (b) The quality ratios of the advanced cybersecurity topics using proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS). (c) The correlation between the number of users and the time consumed when solving basic cybersecurity tasks with the proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS).

This ratio shows the final cybersecurity awareness levels of the tested users. Consequently, we analyze the correlation between the time and the quality ratio. The result demonstrates in Figure 4b that the proposed WBCA has a 99.97% quality ratio. Whereas, the contending models have a 98.08-99.38% quality ratio. M-TISM has a lower quality ratio. The main reason for not completing tasks is that the contending models are affected due to malicious threats compared to the proposed WBCA model.

### 6.2.3. User Response Time

It refers to an important measurement indicator that demonstrates how much time the user gets for the task completion. It is the time that is required to complete the given cybersecurity tasks. Two different experiments are conducted. In the first experiment, time is measured for the basic cybersecurity tasks. In the second experiment, time is measured for the advanced tasks. Therefore, the basic task is calculated as:

$$C_{bt} = \frac{n_u}{t_w} \times 100\% \quad (40)$$

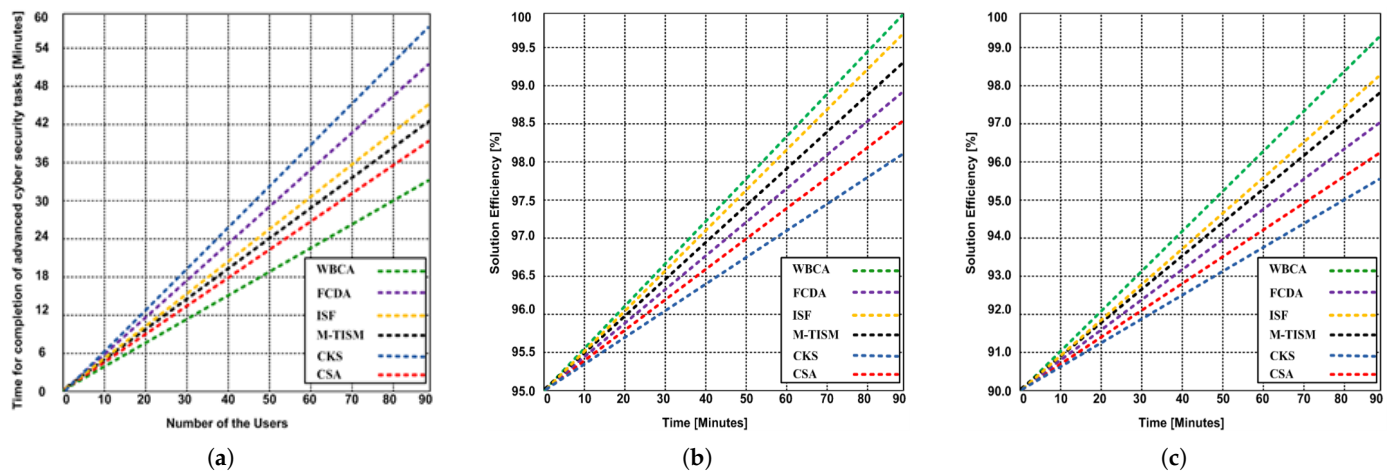
where  $C_{bt}$  is the correlation between the number of users and time wasted when solving basic cybersecurity tasks;  $n_u$  is the number of users; and  $t_w$ : is the time wasted when solving basic cybersecurity tasks.

Based on the result, we determine that a maximum of 90 users complete their basic cybersecurity tasks in 29.58 minutes with the proposed WBCA model. Whereas M-TISM, ISF, FDCA, CSA, and CKS help the users to complete their tasks in 39.58, 37.31, 35.01, 32.41, and 49.59 minutes respectively. In the second experiment, the proposed WBCA model takes 33.01 minutes to help the 90 users to complete their advanced cybersecurity tasks, while the contending models M-TISM, ISF, FDCA, CSA, and CKS support the users to finish their advanced cybersecurity tasks in 42.05, 45.01, 51.09, 39.03 and 57.23 respectively.

### 6.2.4. Solution Efficiency

Two experiments have been conducted to determine the solution efficiency. In the first experiment, the solution efficiency of the basic cybersecurity tasks is determined. In the second experiment, the solution efficiency of the advanced cybersecurity tasks is identified. The solution efficiency of the basic tasks is calculated as:

$$S_{eb} = \frac{t_b}{n_b} \times 100\% \quad (41)$$



**Figure 5.** (a) The correlation between the number of users and the time consumed when solving advanced cybersecurity tasks with the proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS). (b) The solution efficiency of the proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS) using the basic cybersecurity tasks. (c) The solution efficiency of the proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS) using the advanced cybersecurity tasks.

where  $S_{eb}$  is the solution efficiency of the basic tasks;  $n_b$  is the number of basic cybersecurity tasks; and  $t_b$  is the wasted time to solve these basic cybersecurity tasks.

Figure 4c shows the solution efficiency of the proposed WBCA and contending state-of-the-art models. The results demonstrate that the solution efficiency of the proposed WBCA is found to be 100%, while the solution efficiency of the contending model is 98.06-99.65%. Based on the result, we conclude that the proposed WBCA model is working efficiently. On the other hand, the contending models reduce the solution efficiency. The CKS model is highly affected as compared to other contending models. When we conduct the second experiment with the advanced cybersecurity tasks, the performance of the proposed WBCA is slightly reduced despite it gets 99.34% that is much higher than contending models depicted in Figure 5a. Based on the results, we observed that the contending models show a lower solution efficiency of 95.48-98.12%. The CKS is again producing lower solution efficiency.

Hence, the solution efficiency of the advanced tasks is calculated as:

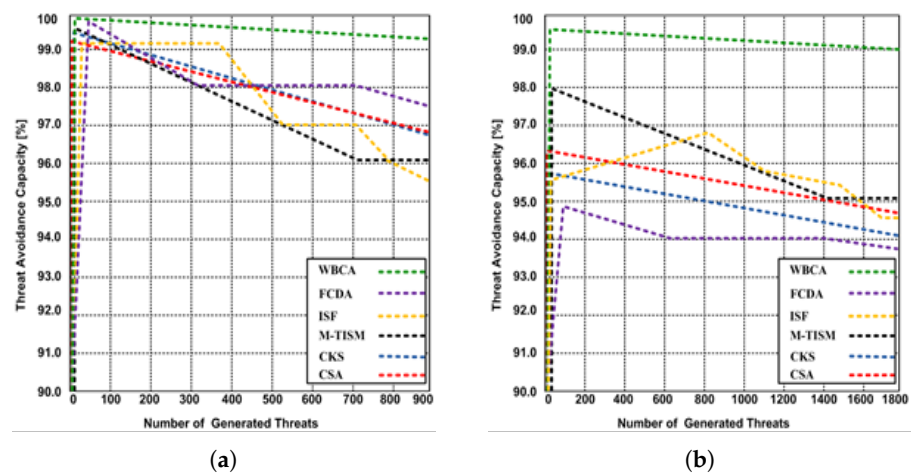
$$S_{ea} = \frac{t_a}{n_a} \times 100\% \quad (42)$$

where  $S_{ea}$  is the solution efficiency of the advanced tasks,  $n_a$  is the number of advanced cybersecurity tasks, and  $t_a$  is the time wasted when solving these advanced cybersecurity tasks.

#### 6.2.5. Threat Avoidance Capacity

The model can eliminate the malicious activities and exposures that negatively affect the performance of the model. Here, different scenarios are generated to determine the threat avoidance effectiveness of the proposed WBCA and competing models. In Figure 6a, a maximum of 900 different types of threats (Denial of Service, Man-in-the-Middle, Malware, Phishing, and spam) have been generated. The result demonstrates that the proposed WBCA has a 99.32% threat avoidance capacity, whereas the contending models have 95.52-97.72% threat avoidance capacity. ISF shows the lower 95.52% threat avoidance capacity as compared to other contending models.

When the number of threats is maximized up to 1800, the threat avoidance capacity of the proposed WBCA is not highly affected. Despite the increase in the number of threats, the proposed WBCA shows 99.11% threat avoidance capacity. On the other hand, the contending models are highly affected by maximizing the number of threats. The



**Figure 6.** (a) Threat avoidance capacity of the proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS) with maximum 900 threats. (b) Threat avoidance capacity of the proposed WBCA and contending models (M-TISM, ISF, FDCA, CSA and CKS) with maximum 1800 threats.

contending models show the threat avoidance capacity of 93.81-95.04% depicted in Figure 6b. The main reason for getting the higher threat avoidance capacity is to use Blockchain technology that greatly reduces the potential threats.

6.3. Result Discussion

The proposed WBCA model consists of several program modules. The first module is responsible for defining the primary cybersecurity awareness outcome. The second module is responsible for deriving the result of the initial check, which ensures the information security knowledge of the user. Since the simple counting sort algorithm is used for verification, the program does not require significant resources, and the user does not need a powerful technique to use it. Moreover, the proposed WBCA model uses Blockchain technology to avoid any potential threat. The proposed WBCA shows higher performance than competing models (M-TISM, ISF, FDCA, CSA, and CKS) from the perspective of consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity shown in Table 2. The proposed WBCA makes it possible to easily determine what level of information security awareness a person has. Regardless of the result, the program hints at the shortcomings of the user in terms of the testing errors and gives recommendations for studying the relevant information security topics. Additionally, a big plus for the user is that the program is free, has an open license, and will always be available for download and further use. If there are sudden problems while using this program, the user can always leave feedback through the developer’s email. However, it is worth noting a couple of disadvantages regarding this program. This program only checks the basic information security awareness level of the user. At the moment, the program is not intended for advanced information security awareness testing. However, this drawback is insignificant, and in the future, people can always add an extended database of advanced questions to it. In the end, we can say that an effective program has been created to identify the current level of information security awareness possessed by any individual.

**Table 2.** Comparative Analysis of the proposed WBCA and contending models: (M-TISM, ISF, FDCA, CSA and CKS).

Models	Consistency	Quality Ratio	User Response Time in minutes (Basic Task)	User Response Time in minutes (Advanced Task)	Efficiency (Basic Task)	Efficiency (Advanced Task)	Threat Avoidance (900 Threats)	Threat Avoidance (1800 Threats)
M-TISM	98.0%	98.08%	39.58	42.05	99.26%	97.01%	96.06%	95.04%
ISF	98.75%	98.61%	37.31	45.01	99.65%	98.12%	95.52%	98.17%
FDCA	98.17%	99.38%	37.31	51.09	98.88%	97.85%	97.72%	93.81%
CSA	98.37%	98.39%	32.41	39.03	98.52%	96.11%	96.92%	96.16%
CKS	97.4%	98.78%	49.59	57.23	98.06%	95.48%	96.92%	95.54%
<b>WBCA</b>	<b>99.76%</b>	<b>99.97%</b>	<b>29.58</b>	<b>33.01</b>	<b>100 %</b>	<b>99.34%</b>	<b>99.32%</b>	<b>99.11%</b>

## 7. Conclusions

This paper introduces a novel WBCA model for promoting high cybersecurity awareness among users. The proposed WBCA works via three modules. The user is tested on common cybersecurity questions and tasks, such as email phishing and weak password policies, and then the program checks if the user has good basic knowledge by making tests regarding advanced cybersecurity topics. The advantage of the proposed WBCA model is the strong check for current cybersecurity trends in the usual process of user behavior. This helps to determine if the person sufficiently cybercrime resistant. The effectiveness of the proposed WBCA is tested on different metrics (consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity) and compared to the state-of-the-art models. The comparative analysis with several topics regarding typical cybercriminal attacks on the users is performed. The proposed WBCA shows higher consistency, quality ratio, user response time, solution efficiency, and threat avoidance capacity than the contending models (M-TISM, ISF, FDCA, CSA and CKS). Based on the results, it is proved that WBCA is a good choice for testing if the current information security basics are sufficient to ensure that the person will minimize the risk of being a cybercrime victim. In the future, we will conduct advanced information security awareness testing. Additionally, we will also add an extended database of advanced questions to it.

**Author Contributions:** .

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Mittal, A., Gupta, M. P., Chaturvedi, M., Chansarkar, S. R., & Gupta, S. Cybersecurity Enhancement through Blockchain Training (CEBT)—A serious game approach. *International Journal of Information Management Data Insights* **2021**, 1, 1, 100001.
2. Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access* **2019**, 7, 168774-168797.
3. Kaur, J., & KR, R. K. The Recent Trends in CyberSecurity: A Review. *Journal of King Saud University-Computer and Information Sciences* **2021**.
4. Ventures, C. *Cybersecurity jobs report*, **2017**, Herjavec Group.
5. Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in human behavior* **2021**, 120, 106745.
6. Borkovich, Debra J., and Robert Joseph Skovira. "CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: WHO'S WORSE, EMPLOYEES OR HACKERS?." *Issues in Information Systems* **2019**, 20.3.
7. Frank, Michele L., Jonathan H. Grenier, and Jonathan S. Pyzoha. "Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework." *Journal of Accounting and Public Policy* **2021**, 106860.
8. Button, Mark, and Jack Whittaker. "Exploring the voluntary response to cyber-fraud: From vigilantism to responsabilisation." *International Journal of Law, Crime and Justice* **2021**, 66, 100482.
9. Almiani, Muder, et al. "Deep recurrent neural network for IoT intrusion detection system." *Simulation Modelling Practice and Theory* **2020**, 101, 102031.
10. Aberbach, Joel D., and Tom Christensen. "Academic autonomy and freedom under pressure: Severely limited, or alive and kicking?." *Public Organization Review* **2018**, 18.4, 487-506.



11. George, Jordana J., and Dorothy E. Leidner. "From clicktivism to hacktivism: Understanding digital activism." *Information and Organization*, **2019**, 29.3, 100249.
12. Anderson, Ross, Chris Barton, Rainer Böhlme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. *Measuring the changing cost of cybercrime*. **2019**.
13. Nouh, Mariam, Jason RC Nurse, Helena Webb, and Michael Goldsmith. "Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement." *arXiv preprint arXiv:1902.06961* **2019**.
14. Yar M., Steinmetz K. F. *Cybercrime and society*. – *SAGE Publications Limited* **2019**.
15. Shuftipro. Available online: <https://shuftipro.com/blog/how-age-verification-protects-the-e-commerce-industry-from-potential-risks/> (accessed on 3 July 2021).
16. Nurse, Jason RC. Cybercrime and you: How criminals attack and the human factors that they seek to exploit, *arXiv preprint arXiv:1811.06624*, **2018**.
17. Lane, Ben R., Paul M. Salmon, Dennis Desmond, Adrian Cherney, Adam Carley, Adam Hulme, and Neville A. Stanton. "Out of control? Using STAMP to model the control and feedback mechanisms surrounding identity crime in darknet marketplaces." **2020** *Applied Ergonomics* **89**, 103223.
18. Bello, Muktar, and Marie Griffiths. "Routine activity theory and cybercrime investigation in Nigeria: how capable are law enforcement agencies?." *In Rethinking Cybercrime* **2021**, pp. 213-235. Palgrave Macmillan, Cham.
19. Umanailo, M. Chairul Basrun, Imam Fachruddin, Deviana Mayasari, Rudy Kurniawan, Dewien Nabelah Agustin, Rini Ganefwati, Pardamean Daulay et al. "Cybercrime Case as Impact Development of Communication Technology That Troubling Society." *Int. J. Sci. Technol. Res* **2021**, 8, no. 9, 1224-1228.
20. Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. "National initiative for cybersecurity education (NICE) cybersecurity workforce framework." *NIST special publication* **2017** 800, no. 181.
21. Pessim, Paulo SP, and Márcio J. Lacerda. "State-feedback control for cyber-physical LPV systems under DoS attacks." *IEEE Control Systems Letters* **2020**, 5, no. 3, 1043-1048.
22. Talukder, Md Arabin Islam, Hossain Shahriar, and Hisham Haddad. "Point-of-sale device attacks and mitigation approaches for cyber-physical systems." *In Cybersecurity and Privacy in Cyber-Physical Systems* **2019**, pp. 367-391. CRC Press.
23. Dreyfuss, Rochelle Cooper. "TRIPS-Round II: Should Users Strike Back?." *In The Regulation of Services and Intellectual Property*, **2017**, pp. 397-411. Routledge.
24. Eskandari, Shayan, Andreas Leoutsarakos, Troy Mursch, and Jeremy Clark. "A first look at browser-based cryptojacking." *In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, **2018**, pp. 58-66. IEEE.
25. Burlison, Jonathan D., Susan D. Scott, Emily K. Browne, Sierra G. Thompson, and James M. Hoffman. "The second victim experience and support tool (SVEST): validation of an organizational resource for assessing second victim effects and the quality of support resources." *Journal of patient safety* **2017**, 13, no. 2, 93.
26. Cascavilla, Giuseppe, Damian A. Tamburri, and Willem-Jan Van Den Heuvel. "Cybercrime Threat Intelligence: a Systematic Multi-Vocal Literature Review." *Computers & Security* **2021**, 102258.
27. Tsakalidis, George, and Kostas Vergidis. "A systematic approach toward description and classification of cybercrime incidents." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2017**, 49, no. 4, 710-729.
28. Senarak, Chalermpong. "Port cybersecurity and threat: A structural model for prevention and policy development." *The Asian Journal of Shipping and Logistics* **2021**, 37, no. 1, 20-36.
29. D'hooge, Laurens, Tim Wauters, Bruno Volckaert, and Filip De Turck. "In-depth comparative evaluation of supervised machine learning approaches for detection of cybersecurity threats." *In 4th International Conference on Internet of Things, Big Data and Security (IoTBDs)*, 2019, pp. 125-136.
30. Gallo, Luigi, Alessandro Maiello, Alessio Botta, and Giorgio Ventre. "2 Years in the anti-phishing group of a large company." *Computers & Security* **2021**, 105 102259.
31. Brilingaitė, Agnė, Linas Bukauskas, and Aušrius Juozapavičius. "A framework for competence development and assessment in hybrid cybersecurity exercises." *Computers & Security* **2020**, 88, 101607.
32. Kam, Hwee-Joo, Philip Menard, Dustin Ormond, and Robert E. Crossler. "Cultivating cybersecurity learning: an integration of self-determination and flow." *Computers & Security* **2021**, 96 101875.
33. Rajan, Rishabh, Nripendra P. Rana, Nakul Parameswar, Sanjay Dhir, and Yogesh K. Dwivedi. "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management." *Technological Forecasting and Social Change* **2021**, 170, 120872.
34. Švábenský, Valdemar, Pavel Čeleda, Jan Vykopal, and Silvia Brišáková. "Cybersecurity knowledge and skills taught in capture the flag challenges." *Computers & Security* **2021**, 102, 102154.
35. Hart, Stephen, Andrea Margheri, Federica Paci, and Vladimiro Sassone. "Riskio: A serious game for cyber security awareness and education." *Computers & Security* **2020**, 95, 101827.