Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ

Programa de Pós-Graduação em Ciência da Computação

PROCESSO SELETIVO 2018.3

PROVA DE LÍNGUA INGLESA

INSTRUÇÕES GERAIS AOS CANDIDATOS

- O tempo total para realização das provas é de **1 hora** ***(1h)***.
- Ao término da prova, o candidato deverá devolver o cartão resposta.
- É imprescindível verificar no cartão resposta o número de inscrição do candidato no espaço reservado para tal.

  A IDENTIFICAÇÃO DOS CANDIDATOS EM TODAS AS PÁGINAS DEVERÁ SER FEITA **APENAS** PELO NÚMERO DE INSCRIÇÃO.
- As respostas deverão ser transpostas para o cartão resposta com caneta de tinta azul ou preta. Não serão consideradas as respostas que não estiverem transcritas no cartão resposta, bem como não serão consideradas respostas rasuradas.
- A Prova de Língua Inglesa é constituída por 10 questões objetivas.
- Cada questão objetiva tem somente uma resposta correta.
- A prova deve ser feita sem consulta e sem empréstimo de material.
- Verifique se sua prova contém 10 questões, assim como o cartão de respostas.
- **Não** é permitido o uso de calculadora, celular ou qualquer outro aparelho durante a realização da prova. É vedado o empréstimo de qualquer material entre os candidatos.

Boa Prova !

Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ

Programa de Pós-Graduação em Ciência da Computação

PROCESSO SELETIVO 2018.3

PROVA DE LÍNGUA INGLESA

CARTÃO DE RESPOSTAS

INSCRIÇÃO Nº: ___

Questão	Alternativa			
1	A	B	C	D
2	A	B	C	D
3	A	B	C	D
4	A	B	C	D
5	A	B	C	D
6	A	B	C	D
7	A	B	C	D
8	A	B	C	D
9	A	B	C	D
10	A	B	C	D

Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ

Programa de Pós-Graduação em Ciência da Computação

PROCESSO SELETIVO 2018.3

PROVA DE LÍNGUA INGLESA

TEXT 1

Researcher exposing fake news with computer coding

Computer scientist Sherif Saad says fake news is a major international problem that is continuing to grow, but help is on the way.

A computer detection model he helped to design can identify a fake news story with up to 98 per cent accuracy.

"Fake news is getting more scientifical attention, especially in the wake of the 2016 U.S. presidential election, when we saw fake news stories shared millions of time on social media," says Dr. Saad, computer science professor.

"We are teaching the computer to distinguish between truth and fiction by giving it known examples, real and fake, until the algorithm develops sensors so it can work on its own in the future," he says.

Saad and his research team started by feeding articles that have already been deemed real or fake, into a computer program and wrote an algorithm to create "learning models." Essentially, they are teaching the computer model how to analyze, interpret and predict which stories are true, and which are false.

These machine learning techniques created an algorithm that, in future, can be fed stories on the learned topic, to successfully pick out fake news from legitimate stories. The team started with a combination of news articles from different years with a broader variety of political topics.

"We collected our data set of fake and real articles and limited the scope to revolve around the 2016 US elections and the articles that discuss topics around it. In total, we picked 2,000 articles: 1,000 fake articles and 1,000 real articles," he says.

"Our model achieved upwards of 98 per cent accuracy when using this type of data. This is a popular but complicated research area and with our model, we've had amazing results."

Their model can now accurately identify a fake news story about elections, however, Saad says at this point it cannot distinguish stories on other topics. That would require retraining with a new set of articles.

"At this point we can't design a general news detector, so we must train it for a specific type of story," says Saad. "It's all about context."

"It is expensive and time-consuming to train the program. It can be updated to follow an election from 2008 or 2016, but we need to make a general model that could switch between any topic and didn't require learning — that is the next goal."

Saad co-authored the paper Detection of Online Fake News Using N-Gram Analysis and Machine Learning Techniques, published as part of a conference notes series from the International Conference on Intelligent, Secure and Dependable Systems in Distributed and Cloud Environments.

(Adaptedfromhttp://www.uwindsor.ca/dailynews/2018-02-16/researcher-exposing-fake-news-computer-coding)

Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ

Programa de Pós-Graduação em Ciência da Computação

PROCESSO SELETIVO 2018.3

PROVA DE LÍNGUA INGLESA

Answer questions 1 to 4 according to TEXT 1.

1. According to Text 1, it is CORRECT to say that

A. the last U.S. presidential election was the trigger for more research on how to debunk fake news.

B. Saad has achieved results in detecting fake news that had never seen before.

C. the algorithm developed by Saad is in the limelight once it can work on its own.

D. Saad has been facing difficulties in his research once he works all by himself.

2. O algoritmo criado por Saad,

A. é capaz de identificar *fake news* sobre apenas dois assuntos.

B. é alimentado tanto de notícias verdadeiras quanto de notícias falsas.

C. ainda não apresentou resultados que tenham deixado o cientista satisfeito.

D. no futuro, será capaz de identificar *fake news* também em vídeos.

3. Which of the following statements is/are correct according to Text 1?

I the model created by Saad is useful for identifying fake news about elections.

II Saad aims at not having to teach the computer to distinguish between truth and fiction in the future.

III Saad hasn't published his findings yet, but it will be done in a book.

A. I

B. II

C. I e II

D. II e III

4. Em "These machine learning techniques created an algorithm that, in future, can be fed stories on the learned topic..." (6^o parágrafo), machine learning techniques pode ser traduzido por

A. máquinas aprendizes de técnicas.

B. técnicas de máquinas aprendizes.

C. técnicas de aprendizado da máquina.

D. aprendizado técnico da máquina.

TEXT 2

Future Wireless Systems for Human Bond Communications (HBC)

WBAN

Nowadays the digitalization of human perceptions and sensations, so that this new very personal information can be shared, is a frontier of ICT. Imagine the future: every human being carrying one or more sensors that sense or reveal a very personal information, when this information is created by the body, such as tasting a delicious food, touching a new irregular surface, looking at the preferred color or watching something horrible, could be only an infinitesimal part of the perception and sensations that the body generates in our everyday life.

In order to digitalize this new kind of information, a wearable device is required. The device will be capable of revealing the information, transforming it into a digital content and sending it through a communication channel. Thus, the concept is that the humans have to carry a so-called body area network (BAN), which detects and then transmits the information. Due to the mobility issue, the information is usually sent by a wireless link. Moving personal health data has a very similar security issues of HBC data, since both are very private and must not be modified or accessed by not-authorized personnel.

As an example in the healthcare context, the evolution of WBAN will go towards the human bond communications.

The WBAN has emerged as a new technology for e-healthcare that allows the data of a patient's vital parameters and movements to be collected by small wearable or implantable sensors and communicated using wireless links. WBAN technology has great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems.

The benefits of WBAN are many, but mainly this one: instead of being measured face-to-face, patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information can be then shared and accessed by various authorized users such as healthcare staff, care-givers, researchers, government agencies and insurance companies.

Since the person-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of this data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments. Therefore, it is extremely important to protect patient-related data against malicious modification and, at the same time, to ensure the reliability and dependability of the data. Protection issue ranges from data stored inside the on/in-body device to the transmission of data to the off-body network.

To design data security and privacy mechanisms for WBANs means to find balances between security, efficiency and usability. Stringent resource constraints on WBAN devices, e.g., the sensor nodes, basically require the security mechanisms to be as lightweight as

possible. As expected, the security design to let HBC become real is a hard task, since security mechanisms must be at the same time:

- robust but lightweight,
- low latency but dependable,
- unbreakable but simple.

In the HBC vision, the data are not health-related but still has the same importance, since they represent the senses and sensations of an individual. This kind of data can lead to a superior profile of a subject, much more than today algorithms exploiting the "Internet life" of an individual. Such superior profiles are pure gold for companies that today spend millions of dollars to buy customers profiles from big digital industries, such as Google, Facebook, etc.

Security and Resilience

The HBC will happen to operate in open-access environments, which means that they can also accommodate attackers. The open wireless channel makes the data prone to being eavesdropped, modified as well as jammed. Together with threats to stored data, other threats can come from the device compromise as well as from the network dynamic.

The sensor nodes worn by a HBC user are subjected to compromise, since they can be usually easily taken and opened or tampered. If data is directly encrypted and stored in a node along with its encryption key, the compromise of this node will lead to the disclosure of the data. Also, local servers may not be trustworthy, since malicious people can either attack it remotely from Internet, or simply go physically to the room where a HBC user is and wait for the chance to compromise the local server.

Besides, the HBC network dynamic is highly time-variant, i.e. nodes may join or leave the network frequently. Nodes may leave out due to battery low or due to a malicious attack. Other types of attacks may easily replace legitimate nodes with faked sensors and take away legitimate nodes with data inside. The personal-related data, if not well kept in more than one node, could be lost easily due to the network dynamics. Moreover, false data could be injected or treated as legitimate due to lack of authentication.

All these possible threats lead to stringent requirements when building the security of HBC.

(Abridgedfromhttps://pdfs.semanticscholar.org/b23f/7c35dcdcd3c1972f983371812abf3ab2435a.pdf)

Answer questions 5 to 10 according to TEXT 2:

5. According to Text 2, it is CORRECT to say that

A. WBAN won't surpass HBC, but it's been of great value for healthcare.

B. Although WBAN is an important technology for healthcare, it still has a narrow range of uses.

C. The WBAN technology allows sensors to gather important information about a patient's health.

D. WBAN needs to improve the speed it sends patients' information to medical databases.

6. Which option does NOT hold a linking word that conveys the idea of ADDITION?

A. "**Therefore**, it is extremely important to protect patient-related data against malicious modification and, at the same time, to ensure the reliability and dependability of the data." (6th paragraph)

B. "**Also**, local servers may not be trustworthy, since malicious people can either attack it remotely from Internet, or simply go physically to the room where a HBC user is and wait for the chance to compromise the local server." (10th paragraph)

C. "**Besides**, the HBC network dynamic is highly time-variant, i.e. nodes may join or leave the network frequently." (11th paragraph)

D. "**Moreover**, false data could be injected or treated as legitimate due to lack of authentication." (11th paragraph)

7. Segundo o texto 2,

A. as informações enviadas pelo WBAN para as bases médicas não podem ser acessadas por qualquer pessoa, já que a rede é fechada e segura.

B. caso haja falhas no acesso às informações médicas armazenadas no WBAN, o tratamento do paciente pode ser comprometido.

C. o grande problema dos sensores usados por pacientes é eles ainda serem mais pesados e maiores do que os pesquisadores gostariam.

D. os dados dos perfis dos indivíduos gerados pela tecnologia HBC não é muito diferente das informações obtidas pelos algoritmos.

8. The suffix *–ING* is NOT forming a verb in

A. "Imagine the future: every human **being** carrying one or more sensors..." (1st paragraph)

B. "...instead of **being** measured face-to-face, patients' health-related parameters..." (5th paragraph)

C. "...correct medical data will possibly prevent a patient from **being** treated effectively..." (6th paragraph)

D. "The open wireless channel makes the data prone to **being** eavesdropped,..." (9th paragraph)

9. In "The HBC will happen to operate in open-access environments, which means that they can also accommodate attackers." (9th paragraph), the relative pronoun which refers to

A. environments.

B. open-access environments.

C. they can also accommodate attackers.

D. the HBC will happen to operate in open-access environments.

10. Acerca da segurança do HBC, NÃO é correto afirmar que

A. os dados armazenados correm o risco de ficar expostos.

B. servidores locais não são confiáveis, pois podem sofrer ataques remotos.

C. dados falsos podem ser tratados como reais por falta de autenticação.

D. os sensores são frágeis e podem se quebrar facilmente.