Revisar envio do teste: Semana 5 - Atividade Avaliativa

Usuário	LIZIS BIANCA DA SILVA SANTOS
Curso	Protocolos de Comunicação IoT - COM380 - Turma 001
Teste	Semana 5 - Atividade Avaliativa
Iniciado	13/11/24 20:04
Enviado	13/11/24 20:13
Data de vencimento	15/11/24 23:59
Status	Completada
Resultado da tentativa	10 em 10 pontos
Tempo decorrido	9 minutos
Instruções	Olá, estudante! 1. Para responder a esta atividade, selecione a(s) alternativa(s) que você considerar correta(s); 2. Após selecionar a resposta correta em todas as questões, vá até o fim da página e pressione "Enviar teste". 3. A cada tentativa, você receberá um novo conjunto de questões diferentes para que você responda e tente alcançar melhores resultados. Pronto! Sua atividade já está registrada no AVA.
Resultados exibidos	Todas as respostas, Respostas enviadas, Respostas corretas, Comentários, Perguntas respondidas incorretamente

Pergunta 1

1,45 em 1,45 pontos

A tecnologia da internet das coisas notabiliza-se por tangibilizar no mundo físico o valor inerente às tecnologias da informação. Afinal, é pelo arranjo combinado de sensores e atuadores junto às diversas redes computacionais que se consegue detectar o que se passa no mundo físico, entregando tais leituras para o devido processamento dos algoritmos de *software*, calculando os resultados com base nas leituras e, finalmente, direcionando os atuadores a utilizar tais cálculos para que se modifique o mundo físico em algum aspecto.

Sobre o que foi apresentado, analise as asserções a seguir e as relações propostas entre elas.

I. O mais comum é que as redes formadas pelas "coisas" do IoT (entre sensores e atuadores) sejam de circuito fechado.

PORQUE

II. É necessário um número surpreendentemente diminuto de sensores e atuadores para executar funções simples da IoT.

Analisando as asserções anteriores conclui-se que:

Resposta Selecionada: b. a primeira asserção é verdadeira e a segunda é falsa.

Respostas:
a. as duas asserções são verdadeiras e a segunda não justifica a primeira.
b. a primeira asserção é verdadeira e a segunda é falsa.
c. as duas asserções são falsas.
as duas asserções são verdadeiras e a segunda justifica a primeira.
d.
e. a primeira asserção é falsa e a segunda é verdadeira.

Comentário da resposta: **JUSTIFICATIVA**

A asserção I é verdadeira, pois geralmente as redes IoT são do tipo circuito fechado, o que significa que o parâmetro físico que um atuador tem controle é prontamente lido de volta naquele sistema por meio de um sensor, encerrando, dessa forma, um *loop* contínuo em tempo real e permitindo o monitoramento e o controle estrito dos processos que ocorrem no âmbito físico. A asserção II é falsa, porque o número de sensores e atuadores para executar até as funções mais simples da IoT é surpreendentemente *grande* (e não diminuto), inclusive para as mais triviais atividades.

Pergunta 2

1,45 em 1,45 pontos

A organização e a análise de uma solução IoT podem se dar a partir de um modelo de quatro camadas, sendo essas a de sensor e rede, de gateway e rede, de *middleware* e de aplicação. Quanto à camada de sensor e rede, é ali que se "sente" alguma grandeza do meio físico, obtendo-se uma informação de um objeto real, e enviando-a para um dispositivo externo para posterior tratamento.

Sobre o que foi apresentado, analise as asserções a seguir e as relações propostas entre elas.

I. A camada de sensor e rede realiza o envio de informações para outro sistema usando tecnologias de *blockchain* e *torrent*.

PORQUE

II. É facultado o uso de redes sem fio (*wireless*) para o emprego de dispositivos e sensores na camada de sensor e rede.

Analisando as asserções anteriores, conclui-se que:

Resposta Selecionada: e. a primeira asserção é falsa e a segunda é verdadeira.

Respostas:
a. as duas asserções são verdadeiras e a segunda justifica a primeira.
a.
as duas asserções são verdadeiras e a segunda não justifica a primeira.
b.
a primeira asserção é verdadeira e a segunda é falsa.
c.
as duas asserções são falsas.
d.
a primeira asserção é falsa e a segunda é verdadeira.
e.

Comentário da resposta: **JUSTIFICATIVA**

A asserção I é falsa, pois a camada de sensor e rede obtém informações do meio físico mediante leituras de etiquetas RFID, QR-codes, códigos de barra ou dos mais diversos tipos de sensores e faz o envio dessas informações para outro sistema usando tecnologias de redes locais (como *wi-fi* e Ethernet) ou de redes pessoais (como *ZigBee*, *bluetooth*, infravermelho etc.), não envolvendo, portanto, tecnologia de *blockchain* e *torrent*.

A asserção II é verdadeira, pois, na camada de sensor e rede, os dispositivos ou sensores precisam estar conectados, sendo que isso pode se dar mediante redes cabeadas ou até por tecnologia sem fio. É admissível, ainda, que um sensor esteja conectado a um dispositivo por barramentos específicos ou também por portas paralelas e seriais.

Pergunta 3

1,42 em 1,42 pontos

No âmbito dos protocolos de comunicação IoT, há um determinado conceito que se notabiliza por ser descrito como o *software* que se situa entre o sistema operacional e as aplicações nele executadas. Trata-se do _____(lacuna 1), que permite a comunicação e o gerenciamento de dados para aplicações _____(lacuna 2).

Escolha a alternativa que preenche as lacunas corretamente.

Resposta Selecionada: c. *Middleware*, distribuídas.

Respostas:
a. *Firmware*, distribuídas.
b. Compilador, centralizadas.
c. *Middleware*, distribuídas.
d. Sensor, centralizadas.
e. Interpretador, distribuídas.

Comentário da resposta: JUSTIFICATIVA

A primeira lacuna é completada pelo termo "*middleware*" e a segunda lacuna é completada pelo termo "distribuídas" pela mesma razão: denomina-se *middleware* o *software* que se situa entre o sistema operacional e as aplicações nele executadas. Além de permitir a comunicação e o gerenciamento de dados para aplicações distribuídas, ele possibilita que os usuários procedam com solicitações como enviar formulários em um *browser* da *web* ou autorizar que o servidor *web* mostre páginas dinâmicas da *web* a partir de informações do perfil de um determinado usuário. Por sua vez, as alternativas "sensor", "*firmware*", "compilador" e "interpretador" aludem a termos tecnicamente inconsistentes com o objeto da questão, em nada relacionados ao caráter intermediador do *middleware* junto ao sistema operacional e às aplicações, razão pela qual são incorretas e devem ser descartadas.

Pergunta 4

1,42 em 1,42 pontos

Middlewares no contexto de IoT possuem diversas funcionalidades, exceto para:

Resposta Selecionada: interoperar protocolos.

Respostas:
processamento distribuído.
consulta de mensagens.
interoperar protocolos.
desenvolver novas aplicações.
processamento paralelo.

Comentário da resposta: A interoperabilidade de protocolos não é uma funcionalidade do middleware, mas de um modo geral de tecnologias como RPC, SOAP etc., que são usadas.

Pergunta 5

1,42 em 1,42 pontos

Leia o seguinte parágrafo e escolha a alternativa que completa corretamente todas as lacunas:

Os _____ incluem um elemento denominado _____ e uma cadeia de processamento de sinal para disponibilizar as leituras brutas para computadores em rede. _____ são dispositivos que convertem uma forma de energia em outra. _____ nos sistemas de IoT captam sinais elétricos e os convertem em algum tipo de saída física.

Resposta Selecionada: sensores, transdutor, transdutores, atuadores

Respostas:
atuadores, transdutor, transdutores, sensores
sensores, transdutor, transdutores, atuadores
transdutores, sensor, transdutores, atuadores
sensores, atuador, transdutores, transdutores
sensores, atuador, atuadores, transdutores

Comentário da resposta: Sensores usam alguns parâmetros físicos e os transformam em sinais elétricos. Atuadores captam sinais elétricos e os convertem em algum tipo de saída física. Transdutores são dispositivos que convertem uma forma de energia em outra.

Pergunta 6

1,42 em 1,42 pontos

Em termos de tecnologia da internet das coisas, há diferentes fases com as quais a interação com mundo físico-cibernético ocorre. Cada uma dessas fases acaba sendo caracterizada por diferentes tecnologias e protocolos que interagem e têm distintos propósitos e funções. Uma dessas fases, por sinal, notabiliza-se por fazer uso de tecnologias como IEEE 802.15.4 e *bluetooth*.

Assinale a alternativa que corresponde à descrição correta da fase em questão:

Resposta Selecionada: c. fase de coleta.

Respostas:
a. fase de transmissão.
b. fase de utilização.
c. fase de coleta.
d. fase de processamento.
e. fase de gestão.

Comentário da resposta: **JUSTIFICATIVA**

De fato, a fase de coleta diz respeito aos procedimentos para a detecção do ambiente físico, a ação de recolher dados físicos em tempo real e de reconstruir uma percepção geral desses dados. Nesse sentido, tecnologias como RFID e sensores fornecem a identificação de objetos físicos e detecção de parâmetros físicos, ao passo que tecnologias como IEEE 802.15.4 e *bluetooth* são responsáveis pela coleta de dados. Por sua vez, as alternativas "fase de transmissão", "fase de processamento", "fase de gestão" e "fase de utilização" aludem a fases que não se notabilizam por explorar IEEE 802.15.4 e *bluetooth*, razão pela qual são incorretas e devem ser descartadas.

Pergunta 7

1,42 em 1,42 pontos

A segurança em IoT deve considerar diversos aspectos que envolvem comunicação e armazenamento de modo que dados possam estar protegidos contra intrusos. A esse respeito, assinale a alternativa correta:

Resposta Selecionada: Gerenciamento de identidade de acesso é um risco à segurança de IoT.

Respostas:
A indústria de um modo geral se mantém desconectada da Internet e por isso está segura contra acessos indevidos a dispositivos, máquinas etc.
Gerenciamento de identidade de acesso é um risco à segurança de IoT.
A segurança em IoT não melhora ou piora com o aumento do número de dispositivos.
O acesso remoto não é um problema de segurança em IoT.
As interfaces de acesso em IoT são seguras por padrão.

Comentário da resposta: Acesso remoto é um problema para a segurança em IoT, pois o controle do dispositivo pode causar diversos danos. A indústria moderna tem cada vez mais se conectado à Internet por meio de dispositivos e novos dispositivos aumentam os riscos à segurança. Há também problemas de segurança em interfaces de acesso como em APIs.