safeassign by Blackboard
(http://safeassign.blackboard.com/)

22346.202120 - SPRING 2021 - EMERGING THREATS & COUNTERMEAS (ITS-834-M50) - FULL TERM

Week 7 Research Paper

on Sat, Feb 27 2021, 8:39 PM

71% highest match
Submission ID: 783d14ec-0b78-475e-b0b9-64a0ae289005

Attachments (1)

Week 7 Assignment.docx **71%**
Word Count: 1,158
Attachment ID: 4063706585

Week 7 Assignment.docx

Running head: RESEARCH PAPER 1

Research Paper 1

Research Paper

02/27/2020

2 **RESEARCH PAPER THE AUTHORS MANAGED TO ADDRESS HOW THE INTERNET OF THINGS (IOT) DEVICES ARE BECOMING UBIQUITOUS WHILE THEIR SERVICES ARE BECOMING PERVASIVE.** Their success is also noticeable and the number of attacks and threats against the internet of things is on the increase. 3

CYBER-ATTACKS ARE NOT ISSUES THAT ARE NEW TO THE INTERNET OF THINGS, BUT AS THE TECHNOLOGY CONTINUES TO BE DEEPLY INTERWOVEN IN OUR LIVES AND SOCIETIES, IT IS NOW BECOMING NECESSARY THAT PEOPLE STEP UP AND TAKE MEASURES REQUIRED AGAINST CYBER THREATS SERIOUSLY. THUS, THERE IS AN URGENCY TO SECURE IOT, WHICH HAS ALSO RESULTED IN THE NEED TO COMPREHENSIVELY UNDERSTAND THE ATTACKS AND THREATS ON THE INFRASTRUCTURE OF IOT. 4 THE AUTHORS HAVE ALSO ATTEMPTED TO CLASSIFY THE TYPES OF THREATS, BESIDES CHARACTERIZE AND ANALYZE INTRUDERS AND CURRENT ATTACKS THAT ARE DEPLOYED AGAINST IOT SERVICES AND DEVICES.

2 MOREOVER, THE RECENT RAPID DEVELOPMENT AND INCREASING GROWTH IN THE USE OF THE INTERNET OF THINGS AND ITS CAPACITY TO OFFER DIFFERENT CATEGORIES OF SERVICES HAVE MADE THE TECHNOLOGY HAVE A HUGE IMPACT ON BUSINESS ENVIRONMENTS AND SOCIAL LIFE AS WELL. 5 GRADUALLY, THE INTERNET OF THINGS HAS PERMEATED ALL ASPECTS OF MODERN HUMAN LIFE LIKE BUSINESS, HEALTHCARE, AND EDUCATION. The technology has made it easy when it comes to the storage of sensitive data or information companies and individuals, product development, financial data transactions, and marketing as well. **6 AGAIN, THE VAST DIFFUSION OF THE CONNECTED DEVICES WITHIN THE SCOPE OF IOT TECHNOLOGY HAS ALSO CREATED AN ENORMOUS DEMAND FOR ROBUST SECURITY AS IT RESPONDS TO THE EVER-GROWING DEMAND FOR BILLIONS OF CONNECTED SERVICES AND DEVICES ACROSS THE WORLD (ABOMHARA & KOIEN, 2015).**

ACCORDING TO THE AUTHORS, THE NUMBER OF THREATS AND ATTACKS IS RISING DAILY AND THEY HAVE BEEN ON THE INCREASE IN BOTH COMPLEXITY AND NUMBER. 5 IT IS NOT ONLY ABOUT THE NUMBER OF POTENTIAL ATTACKERS TOGETHER THE SIZE OF THE NETWORKS GROWING. THE TOOLS THAT ARE AVAILABLE TO POTENTIAL ATTACKERS ARE ALSO INCREASINGLY BECOMING EFFECTIVE, EFFICIENT, AND SOPHISTICATED. 6 IN THAT CASE, WHEN THE IOT IS LOOKING TO

ACHIEVE THE FULLEST POTENTIAL, THERE MUST BE PROTECTION AGAINST VULNERABILITIES AND THREATS.

ABOMHARA AND KOIEN (2015) ALSO DEFINE SECURITY AS THE PROCESS FOR PROTECTING AN OBJECT AGAINST PHYSICAL DAMAGE, THEFT, LOSS, OR UNAUTHORIZED ACCESS BY MAINTAINING HIGH INTEGRITY AND CONFIDENTIALITY OF INFORMATION ABOUT THE OBJECT. Ideally, security is about making information concerning the object available whenever it is needed. **6** **HOWEVER, THERE IS NO SUCH THING AS SECURING THE STATE OF ANY OBJECT, WHERE TANGIBLE OR NOT SINCE NO OBJECT WILL ALWAYS BE IN A PERFECT SECURE STATE (ABOMHARA & KOIEN, 2015). AN OBJECT IS ALSO SECURE IF THE SUBJECTED PROCESS CAN MAINTAIN THE MAXIMUM INTRINSIC VALUE, ESPECIALLY WHEN SUBJECTED TO DIFFERENT CONDITIONS. AGAIN, THE SECURITY REQUIREMENTS IN THE ENVIRONMENT OF THE IOT ARE NOT DIFFERENT FROM THE ONES USED IN ICT SYSTEMS. THEREFORE, ENSURING IOT WILL ALWAYS REQUIRE MAINTENANCE OF THE HIGHEST INTRINSIC VALUE OF BOTH INTANGIBLE AND TANGIBLE ITEMS.** The tangible objects are the IoT devices while the intangible items are the data, information, and services offered through IoT.

The hypothetical questions being tested concerns entail answering questions relating to the threats against the technology of IoT. In that case, it is important to understand IoT as an asset, the principal entities, threat actors, the threats that can affect the assets, and the capability and resource levels possessed by threat actors. The authors also emphasized that it is necessary to understand the mechanism that can be used against threats even if the current designs of IoT and information systems are protected against the threat. **6** **MANY IOT DEVICES ALSO OPERATE WITHOUT BEING ATTENDED BY HUMANS AND THEREFORE, IT IS EASY FOR AN ATTACKER TO GAIN PHYSICAL ACCESS. SOME OF THE IOT COMPONENTS ALSO COMMUNICATE OVER WIRELESS NETWORKS, ESPECIALLY THE ONES THAT ATTACKERS CAN EASILY OBTAIN CONFIDENTIAL DATA OR INFORMATION THROUGH EAVESDROPPING. ANOTHER CHALLENGE IS THAT MANY COMPONENTS OF THE INTERNET OF THINGS CANNOT SUPPORT COMPLEX SECURITY SYSTEMS BECAUSE OF LOW COMPUTING AND POWER RESOURCE CAPABILITIES.**

Furthermore, cyber threats can also be launched against any IoT facilities and assets, thereby causing potential damage or instability of system operation. The consequences include endangering the general populace or causing severe economic damage to users and owners of the facilities or IoT assets (Abomhara & Koien, 2015). 6 **EXAMPLES OF AREAS THAT CAN EASILY BE ATTACKED INCLUDE HOME AUTOMATION SYSTEMS, INCLUDING HEATING SYSTEMS, PHYSICAL SECURITY SYSTEMS, LIGHTING SYSTEMS, AND AIR CONDITIONING. IN THAT CASE, INFORMATION COLLECTED FROM THE SENSORS EMBEDDED IN LIGHTING OR HEATING SYSTEMS CAN INFORM THE INTRUDER WHEN SOMEBODY IS OUT OR AT HOME. AGAIN, CYBER-ATTACKS CAN BE LAUNCHED AGAINST ANY PUBLIC INFRASTRUCTURE SUCH AS UTILITY SYSTEMS - INCLUDING WATER TREATMENT PLANTS AND POWER SYSTEMS.** The objective of the attacker is to stop the electricity or water supply to users of the public infrastructures.

6 **ABOMHARA AND KOIEN (2015) ALSO EMPHASIZED THAT PRIVACY AND SECURITY ISSUES ARE A GROWING CONCERN FOR SUPPLIERS AND USERS IN THEIR SHIFT TOWARDS THE IMPLEMENTATION OF IOT. IT IS ALSO CERTAINLY EASY TO IMAGINE THE AMOUNT OF DAMAGE CAUSED IF THE CONNECTED DEVICES ARE CORRUPTED OR ATTACKED. FOR THAT REASON, IT IS IMPORTANT TO UNDERSTAND THAT THE ADOPTION OF IOT TECHNOLOGY WITHIN OUR BUSINESS ENVIRONMENTS, WORK, OR HOMES OPENS DOORS TO NEW SECURITY ISSUES. SUPPLIES AND USERS ARE ALSO EXPECTED TO BE CAUTIOUS OF SUCH PRIVACY AND SECURITY CONCERNS.**

5 **IN CONCLUSION, ABOMHARA AND KOIEN (2015) CONCLUDED THAT IOT FACES SEVERAL THREATS THAT SHOULD BE RECOGNIZED FOR PROTECTIVE ACTION.** 6 **THEREFORE, THEIR OVERALL GOAL WAS TO IDENTIFY DOCUMENT, AND ASSESS POTENTIAL THREATS, VULNERABILITIES, AND ATTACKS EXPERIENCED BY THE TECHNOLOGY OF THE INTERNET OF THINGS. THEY ALSO PROVIDED AN OVERVIEW OF THE MOST ESSENTIAL IOT SECURITY CHALLENGES AS THE MAIN FOCUS WAS ON THE SECURITY PROBLEMS SURROUNDING THE INTERNET OF THINGS SERVICES AND DEVICES. THEREFORE, SECURITY CHALLENGES LIKE PRIVACY, CONFIDENTIALITY, ENTITY TRUST, AND PRIVACY WERE ALSO IDENTIFIED. THEY SHOWED THAT IN ORDER TO ESTABLISH MORE**

READILY AVAILABLE IOT SERVICES AND DEVICES THAT ARE MORE SECURE, THERE IS A NEED TO ADDRESS PRIVACY AND SECURITY CHALLENGES. THE DISCUSSION CHAMPIONED BY ABOMHARA AND KOIEN (2015) ALSO FOCUSED ON THE CYBER THREATS CONSISTING OF ACTORS, CAPABILITY, AND MOTIVATION FUELED BY THE EXCEPTIONAL CHARACTERISTICS OF CYBERSPACE. THEY ALSO DEMONSTRATED THAT THREATS FROM CRIMINAL GROUPS AND INTELLIGENCE AGENCIES ARE MOST LIKELY TO BE MORE DIFFICULT TO COUNTER THAN WHEN COMPARED TO THE THREATS FROM INDIVIDUAL HACKERS. THE PRIMARY REASON IS THAT THE TARGETS OF INTELLIGENCE AGENCIES AND CRIMINAL GROUPS ARE NOT EASILY PREDICTABLE WHEREAS THE IMPACT OF AN INDIVIDUAL ATTACK IS USUALLY EXPECTED TO BE LESS SEVERE. FINALLY, UPCOMING STANDARDS OF IOT SERVICES AND DEVICES MUST ADDRESS THE SHORTCOMINGS OF CURRENT IOT SECURITY MECHANISMS. THEREFORE, FUTURE WORK SHOULD CONSIDER GAINING A DEEPER UNDERSTANDING OF THE THREATS FACING IOT INFRASTRUCTURE, INCLUDING THE CONSEQUENCES AND LIKELIHOOD OF THREATS AGAINST IOT.

Citations (6/6)

1 Another student's paper

2 Another student's paper

3 https://ccs-nsuk.net/Home/ResourceByYear?Year=2011

4 Another student's paper

5 Another student's paper

6 https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Matched Text

Suspected Entry: **100% match**

Uploaded - Week 7 Assignment.docx **Source -** Another student's paper

UNIVERSITY OF CUMBERLANDS

University of Cumberlands

Suspected Entry: **73% match**

Uploaded - Week 7 Assignment.docx

RESEARCH PAPER THE AUTHORS MANAGED TO ADDRESS HOW THE INTERNET OF THINGS (IOT) DEVICES ARE BECOMING UBIQUITOUS WHILE THEIR SERVICES ARE BECOMING PERVASIVE

Source - Another student's paper

Internet of Things (IoT) devices are rapidly becoming ubiquitous while IoT services are becoming pervasive

Suspected Entry: **70% match**

Uploaded - Week 7 Assignment.docx

MOREOVER, THE RECENT RAPID DEVELOPMENT AND INCREASING GROWTH IN THE USE OF THE INTERNET OF THINGS AND ITS CAPACITY TO OFFER DIFFERENT CATEGORIES OF SERVICES HAVE MADE THE TECHNOLOGY HAVE A HUGE IMPACT ON BUSINESS ENVIRONMENTS AND SOCIAL LIFE AS WELL

Source - Another student's paper

The recent rapid development of the Internet of Things (IoT) [1, 2] and its ability to offer different types of services have made it the fastest growing technology, with huge impact on social life and business environments

Suspected Entry: **74% match**

Uploaded - Week 7 Assignment.docx

CYBER-ATTACKS ARE NOT ISSUES THAT ARE NEW TO THE INTERNET OF THINGS, BUT AS THE TECHNOLOGY CONTINUES TO BE DEEPLY INTERWOVEN IN OUR LIVES AND SOCIETIES, IT IS NOW BECOMING NECESSARY THAT PEOPLE STEP UP AND TAKE MEASURES REQUIRED AGAINST CYBER THREATS SERIOUSLY

Source - https://ccs-nsuk.net/Home/ResourceByYear?Year=2011

Cyber-attacks are not new to IoT, but as IoT will be deeply interwoven in our lives and societies, it is becoming necessary to step up and take cyber defense seriously

Suspected Entry: **79% match**

Uploaded - Week 7 Assignment.docx

THUS, THERE IS AN URGENCY TO SECURE IOT, WHICH HAS ALSO RESULTED IN THE NEED TO COMPREHENSIVELY UNDERSTAND THE ATTACKS AND THREATS ON THE INFRASTRUCTURE OF IOT

Source - https://ccs-nsuk.net/Home/ResourceByYear?Year=2011

Hence, there is a real need to secure IoT, which has consequently resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure

Suspected Entry: **70% match**

Uploaded - Week 7 Assignment.docx

THE AUTHORS HAVE ALSO ATTEMPTED TO CLASSIFY THE TYPES OF THREATS, BESIDES CHARACTERIZE AND ANALYZE INTRUDERS AND CURRENT ATTACKS THAT ARE DEPLOYED AGAINST IOT SERVICES AND DEVICES

Source - Another student's paper

To classify threat types, besides, analyze and characterize intruders and attacks facing IOT devices and services

Suspected Entry: **69% match**

Uploaded - Week 7 Assignment.docx

GRADUALLY, THE INTERNET OF THINGS HAS PERMEATED ALL ASPECTS OF MODERN HUMAN LIFE LIKE BUSINESS, HEALTHCARE, AND EDUCATION

Source - Another student's paper

gradually permeated all aspects of modern human life, such as education, healthcare, and business, involving the storage of sensitive information about

Suspected Entry: **64% match**

Uploaded - Week 7 Assignment.docx

IT IS NOT ONLY ABOUT THE NUMBER OF POTENTIAL ATTACKERS TOGETHER THE SIZE OF THE NETWORKS GROWING

Source - Another student's paper

Not only is the number of potential attackers

Suspected Entry: **63% match**

Uploaded - Week 7 Assignment.docx

THE TOOLS THAT ARE AVAILABLE TO POTENTIAL ATTACKERS ARE ALSO INCREASINGLY BECOMING EFFECTIVE, EFFICIENT, AND SOPHISTICATED

Source - Another student's paper

attackers are also becoming more sophisticated, efficient and effective [6, 7]

Suspected Entry: **62% match**

Uploaded - Week 7 Assignment.docx

IN CONCLUSION, ABOMHARA AND KOIEN (2015) CONCLUDED THAT IOT FACES SEVERAL THREATS THAT SHOULD BE RECOGNIZED FOR PROTECTIVE ACTION

Source - Another student's paper

IoT faces a number of threats that must be recognized for protective action to

Suspected Entry: **67% match**

Uploaded - Week 7 Assignment.docx

AGAIN, THE VAST DIFFUSION OF THE CONNECTED DEVICES WITHIN THE SCOPE OF IOT TECHNOLOGY HAS ALSO CREATED AN ENORMOUS DEMAND FOR ROBUST SECURITY AS IT RESPONDS TO THE EVER-GROWING DEMAND FOR BILLIONS OF CONNECTED SERVICES AND DEVICES ACROSS THE WORLD (ABOMHARA & KOIEN, 2015)

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide [3–5]

Suspected Entry: **89% match**

Uploaded - Week 7 Assignment.docx

ACCORDING TO THE AUTHORS, THE NUMBER OF THREATS AND ATTACKS IS RISING DAILY AND THEY HAVE BEEN ON THE INCREASE IN BOTH COMPLEXITY AND NUMBER

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

The number of threats is rising daily, and attacks have been on the increase in both number and complexity

Suspected Entry: **66% match**

Uploaded - Week 7 Assignment.docx

IN THAT CASE, WHEN THE IOT IS LOOKING TO ACHIEVE THE FULLEST POTENTIAL, THERE MUST BE PROTECTION AGAINST VULNERABILITIES AND THREATS

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Therefore, for IoT to achieve fullest potential, it needs protection against threats and vulnerabilities [8]

Suspected Entry: **70% match**

Uploaded - Week 7 Assignment.docx

ABOMHARA AND KOIEN (2015) ALSO DEFINE SECURITY AS THE PROCESS FOR PROTECTING AN OBJECT AGAINST PHYSICAL DAMAGE, THEFT, LOSS, OR UNAUTHORIZED ACCESS BY MAINTAINING HIGH INTEGRITY AND CONFIDENTIALITY OF INFORMATION ABOUT THE OBJECT

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Security has been defined as a process to protect an object against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed [7, 9]

Suspected Entry: **62% match**

Uploaded - Week 7 Assignment.docx

HOWEVER, THERE IS NO SUCH THING AS SECURING THE STATE OF ANY OBJECT, WHERE TANGIBLE OR NOT SINCE NO OBJECT WILL ALWAYS BE IN A PERFECT SECURE STATE (ABOMHARA & KOIEN, 2015)

Source - https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

According to Kizza [7] there is no thing as the secure state of any object, tangible or not, because no such object can ever be in a perfectly secure state and still be useful

Suspected Entry: **78% match**

Uploaded - Week 7 Assignment.docx

AN OBJECT IS ALSO SECURE IF THE SUBJECTED PROCESS CAN MAINTAIN THE MAXIMUM INTRINSIC VALUE, ESPECIALLY WHEN SUBJECTED TO DIFFERENT CONDITIONS

Source - https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

An object is secure if the process can maintain its maximum intrinsic value under different conditions

Suspected Entry: **79% match**

Uploaded - Week 7 Assignment.docx

AGAIN, THE SECURITY REQUIREMENTS IN THE ENVIRONMENT OF THE IOT ARE NOT DIFFERENT FROM THE ONES USED IN ICT SYSTEMS

Source - https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Security requirements in the IoT environment are not different from any other ICT systems

Suspected Entry: **62% match**

Uploaded - Week 7 Assignment.docx

THEREFORE, ENSURING IOT WILL ALWAYS REQUIRE MAINTENANCE OF THE HIGHEST INTRINSIC VALUE OF BOTH INTANGIBLE AND TANGIBLE ITEMS

Source - https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Therefore, ensuring IoT security requires maintaining the highest intrinsic value of both tangible objects (devices) and intangible ones (services, information and data)

Suspected Entry: **68% match**

Uploaded - Week 7 Assignment.docx

MANY IOT DEVICES ALSO OPERATE WITHOUT BEING ATTENDED BY HUMANS AND THEREFORE, IT IS EASY FOR AN ATTACKER TO GAIN PHYSICAL ACCESS

Source - https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Most IoT devices operate unattended by humans, thus it is easy for an attacker to physically gain

access to them

Suspected Entry: **63% match**

Uploaded - Week 7 Assignment.docx

SOME OF THE IOT COMPONENTS ALSO COMMUNICATE OVER WIRELESS NETWORKS, ESPECIALLY THE ONES THAT ATTACKERS CAN EASILY OBTAIN CONFIDENTIAL DATA OR INFORMATION THROUGH EAVESDROPPING

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Most IoT components communicate over wireless networks where an attacker could obtain confidential information by eavesdropping

Suspected Entry: **66% match**

Uploaded - Week 7 Assignment.docx

ANOTHER CHALLENGE IS THAT MANY COMPONENTS OF THE INTERNET OF THINGS CANNOT SUPPORT COMPLEX SECURITY SYSTEMS BECAUSE OF LOW COMPUTING AND POWER RESOURCE CAPABILITIES

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Most IoT components cannot support complex security schemes due to low power and computing resource capabilities

Suspected Entry: **74% match**

Uploaded - Week 7 Assignment.docx

EXAMPLES OF AREAS THAT CAN EASILY BE ATTACKED INCLUDE HOME AUTOMATION SYSTEMS, INCLUDING HEATING SYSTEMS, PHYSICAL SECURITY SYSTEMS, LIGHTING SYSTEMS, AND AIR CONDITIONING

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Examples include attacks on home automation systems and taking control of heating systems, air conditioning, lighting and physical security systems

Suspected Entry: **91% match**

Uploaded - Week 7 Assignment.docx

IN THAT CASE, INFORMATION COLLECTED FROM THE SENSORS EMBEDDED IN LIGHTING OR HEATING SYSTEMS CAN INFORM THE INTRUDER WHEN SOMEBODY IS OUT OR AT HOME

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

The information collected from sensors embedded in heating or lighting systems could inform the intruder when somebody is at home or out

Suspected Entry: **67% match**

Uploaded - Week 7 Assignment.docx

AGAIN, CYBER-ATTACKS CAN BE LAUNCHED AGAINST ANY PUBLIC INFRASTRUCTURE SUCH AS UTILITY SYSTEMS - INCLUDING WATER TREATMENT PLANTS AND POWER SYSTEMS

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Among other things, cyber-attacks could be launched against any public infrastructure like utility systems (power systems or water treatment plants) [22] to stop water or electricity supply to inhabitants

Suspected Entry: **76% match**

Uploaded - Week 7 Assignment.docx

ABOMHARA AND KOIEN (2015) ALSO EMPHASIZED THAT PRIVACY AND SECURITY ISSUES ARE A GROWING CONCERN FOR SUPPLIERS AND USERS IN THEIR SHIFT TOWARDS THE IMPLEMENTATION OF IOT

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Security and privacy issues are a growing concern for users and suppliers in their shift towards the IoT [23]

Suspected Entry: **90% match**

Uploaded - Week 7 Assignment.docx

IT IS ALSO CERTAINLY EASY TO IMAGINE THE AMOUNT OF DAMAGE CAUSED IF THE CONNECTED DEVICES ARE CORRUPTED OR ATTACKED

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

It is certainly easy to imagine the amount of damage caused if any connected devices were attacked or corrupted

Suspected Entry: **73% match**

Uploaded - Week 7 Assignment.docx

FOR THAT REASON, IT IS IMPORTANT TO UNDERSTAND THAT THE ADOPTION OF IOT TECHNOLOGY WITHIN OUR BUSINESS ENVIRONMENTS, WORK, OR HOMES OPENS DOORS TO NEW SECURITY ISSUES

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

It is well-recognized that adopting any IoT technology within our homes, work, or business environments opens doors to new security problems

Suspected Entry: **65% match**

Uploaded - Week 7 Assignment.docx

SUPPLIES AND USERS ARE ALSO EXPECTED TO BE CAUTIOUS OF SUCH PRIVACY AND SECURITY CONCERNS

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Users and suppliers must consider and be cautious with such security and privacy concerns

Suspected Entry: **68% match**

Uploaded - Week 7 Assignment.docx

THEREFORE, THEIR OVERALL GOAL WAS TO IDENTIFY DOCUMENT, AND ASSESS POTENTIAL THREATS, VULNERABILITIES, AND ATTACKS EXPERIENCED BY THE TECHNOLOGY OF THE INTERNET OF THINGS

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

The overall goal was to identify assets and document potential threats, attacks and vulnerabilities faced by the IoT

Suspected Entry: **76% match**

Uploaded - Week 7 Assignment.docx

THEY ALSO PROVIDED AN OVERVIEW OF THE MOST ESSENTIAL IOT SECURITY CHALLENGES AS THE MAIN FOCUS WAS ON THE SECURITY PROBLEMS SURROUNDING THE INTERNET OF THINGS SERVICES AND DEVICES

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

An overview of the most important IoT security problems was provided, with particular focus on security challenges surrounding IoT devices and services

Suspected Entry: **77% match**

Uploaded - Week 7 Assignment.docx

THEREFORE, SECURITY CHALLENGES LIKE PRIVACY, CONFIDENTIALITY, ENTITY TRUST, AND PRIVACY WERE ALSO IDENTIFIED

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Security challenges, such as confidentiality, privacy and entity trust were identified

Suspected Entry: **82% match**

Uploaded - Week 7 Assignment.docx

THEY SHOWED THAT IN ORDER TO ESTABLISH MORE READILY AVAILABLE IOT SERVICES AND DEVICES THAT ARE MORE SECURE, THERE IS A NEED TO ADDRESS PRIVACY AND SECURITY CHALLENGES

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

We showed that in order to establish more secure and readily available IoT devices and services, security and privacy challenges need to be addressed

Suspected Entry: **66% match**

Uploaded - Week 7 Assignment.docx

THE DISCUSSION CHAMPIONED BY ABOMHARA AND KOIEN (2015) ALSO FOCUSED ON THE CYBER THREATS CONSISTING OF ACTORS, CAPABILITY, AND MOTIVATION FUELED BY THE EXCEPTIONAL CHARACTERISTICS OF CYBERSPACE

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

The discussion also focused upon the cyber threats comprising actors, motivation, and capability fuelled by the unique characteristics of cyberspace

Suspected Entry: **77% match**

Uploaded - Week 7 Assignment.docx

THEY ALSO DEMONSTRATED THAT THREATS FROM CRIMINAL GROUPS AND INTELLIGENCE AGENCIES ARE MOST LIKELY TO BE MORE DIFFICULT TO COUNTER THAN WHEN COMPARED TO THE THREATS FROM INDIVIDUAL HACKERS

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

It was demonstrated that threats from intelligence agencies and criminal groups are likely to be more difficult to defeat than those from individual hackers

Suspected Entry: **66% match**

Uploaded - Week 7 Assignment.docx

THE PRIMARY REASON IS THAT THE TARGETS OF INTELLIGENCE AGENCIES AND CRIMINAL GROUPS ARE NOT EASILY PREDICTABLE WHEREAS THE IMPACT OF AN INDIVIDUAL ATTACK IS USUALLY EXPECTED TO BE LESS SEVERE

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

The reason is that their targets may be much less predictable while the impact of an individual attack is expected to be less severe

Suspected Entry: **70% match**

Uploaded - Week 7 Assignment.docx

FINALLY, UPCOMING STANDARDS OF IOT SERVICES AND DEVICES MUST ADDRESS THE SHORTCOMINGS OF CURRENT IOT SECURITY MECHANISMS

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

It is important for upcoming standards to address the shortcomings of current IoT security mechanisms

Suspected Entry: **74% match**

Uploaded - Week 7 Assignment.docx

THEREFORE, FUTURE WORK SHOULD CONSIDER GAINING A DEEPER UNDERSTANDING OF THE THREATS FACING IOT

Source -
https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

INFRASTRUCTURE, INCLUDING THE CONSEQUENCES AND LIKELIHOOD OF THREATS AGAINST IOT	As future work, the aim is to gain deeper understanding of the threats facing IoT infrastructure as well as identify the likelihood and consequences of threats against IoT