A model proposal for enhancing cyber security in industrial IoT environments

Atdhe Buja, Marika Apostolova, Artan Luma
Faculty of Contemporary Sciences and Technologies, University of South East European (SEEU), Tetovo, Macedonia

Article Info

Article history:

Received Feb 28, 2024
Revised Apr 24, 2024
Accepted May 12, 2024

Keywords:

Countermeasure
Cybersecurity
Industrial IoT
Model
Threats

ABSTRACT

The revolution of the industrial sector in the automated one has happened with the use of the Industrial Internet of things (IIoT). They are providing unprecedented possibilities for connection, and automation. Also, the ubiquitous of IIoT has brought new cyber security challenges, putting sensitive data at risk. This research paper proposes a comprehensive model for enhancing the cyber security of IIoT systems. Our model integrates various countermeasures, including a proactive assessment of security vulnerabilities, examination of identified vulnerabilities, categorizing data, delivery of comprehensive reports, and assurance of effective countermeasures based on a cost-benefit approach, aligned with industry standards and frameworks. The proposed model aims to address the need for the development of robust and resilient cyber security solutions for IIoT environments. This research work introduces the proposed model's main functions, integration, workflow, and references. With this research, we contribute to the enhancement of cyber security in the IIoT environment by proposing a model that assists with proactive assessment, effective response, and informed decision-making. We envision that the proposed model will support industrial organizations in securing their IIoT systems against cyber threats, ultimately have stability and secure industrial operations.

Corresponding Author:

Atdhe Buja
Faculty of Contemporary Sciences and Technologies, University of South East European (SEEU)
Tetovo, Macedonia
Email: ab29762@seeu.edu.mk

1. INTRODUCTION

The emerge of the Industrial Internet of Things (IIoT) has changed the way industry operates, improved processes, and improved the time and quality of products. The fourth industrial revolution as we know it with Industry 4.0 has brought great changes, from the traditional way of Cyber-Physical Systems (CPS) [1]. Along this evolutionary path, arise threats and cyber-attack challenges that require addressing for the operational security of the industry. However, this technological development has brought a related increase in cyber-attacks targeting IIoT systems, causing threats to industrial operations. The research contribution has a particular focus on enhancing the level of cyber security in IIoT and industrial infrastructures, by proposing the cyber security model for IIoT. This research focuses on producing a cyber security model for IIoT that can be used to analyze and test the effect of cyber-attacks on the behavior of the model. This will allow us in the future to detect and prevent cyber-attacks. Now the industrial infrastructure works using IIoT characteristics such as effectiveness, which is known under the category of IoT and which enables the connection of the industrial control system (ICS) with the internet [2]. Moreover, IIoT with industrial infrastructures are exposed to cyber-attacks, thus becoming attractive targets for attackers. Our previous research [3], has sorted out the vulnerabilities and challenges essential to securing the IIoT environment. From the findings, IIoT is undergoing a lack of privacy and vulnerabilities mostly common cyber-attacks followed by malicious code and Denial of Service (DoS). However, uncommon cyber-attacks are constantly on the rise, targeting IIoT industrial systems in parts where security protection is weak or not as required [3]. To achieve sustainable IIoT systems in the face of cyber-attacks, their cyber security must be considered [4], but the demand is to go further from traditional cyber security [5]. Traditional cyber security includes the triangle of confidentiality, integrity, and availability (CIA); authentication, authorization, and accounting (AAA) mechanisms; antivirus solutions, and firewalls. Have shown a lack of protection against advanced cyber threats targeting IIoT infrastructures. Existing approaches to cyber security in IIoT last a challenge against threats and attacks including advanced persistent threats (APT) [3]. While cyber security is more required for IIoT defense, cyber-attacks can manifest various forms, attack surfaces, and vectors.

The main contributors introduce that while IIoT technologies provide meaningful benefits in industrial contexts, they also present unique security exceptions. Traditional security measures are lacking to address these exceptions. The previous work on literature review [3] recognizes various proposed solutions, such as machine learning (ML) algorithms, 5G wireless communication networks, blockchain integration, and intelligent denial-of-service detection frameworks. Yet, challenges remain in the effective implementation of these solutions, and there is a need beyond research to design a proactive approach to cyber security specific to IIoT applications. There are identified areas for improvement, as follows: i) advanced cyber security countermeasures, ii) integration of emerging technologies, iii) mitigating security challenges in IIoT, and iv) proactive countermeasures.

Furthermore, the common architecture of IIoT and its connection with other Information Technology (IT) components within the industrial environment are presented in Figure 1. This figure shows the essential parts of an IIoT architecture in an industrial environment, including sensors, remote terminal units, human-machine interfaces, network communications, and industrial management systems. In recent years, we have experienced critical cyber-attacks that managed to find vulnerabilities in the devices of the IIoT network. Furthermore, attackers use these found vulnerabilities to exploit and continuously find new ones that are used to penetrate as far as possible into networks and infrastructure by getting unauthorized access. IIoT standard architecture-as mentioned in the introduction of this paper, threats, and cyber-attacks that target IIoT in industrial environments are one after the other with a loss of impact. Precisely for this, cyber security assessments need to observe and recognize the state of infrastructure security. In electronic communications, networks, industrial sensors, and the entire infrastructure, security is important, which makes the operation of the system sustainable.

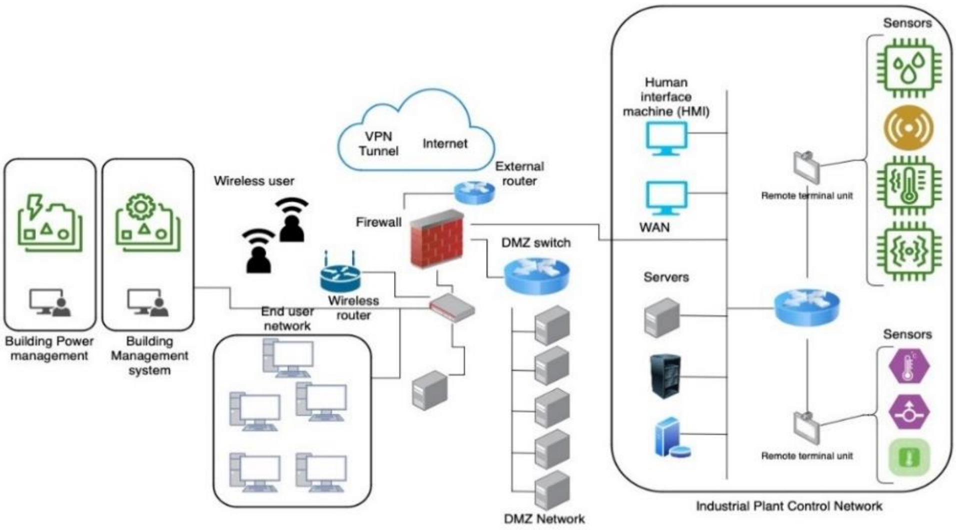
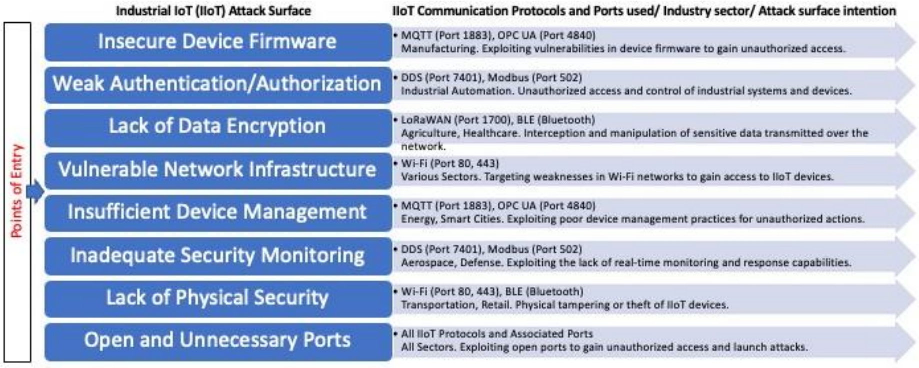


Figure 1. Industrial IoT standard architecture

The proposed model of this paper has the proactive role of cyber security for assessing risk, threats, and vulnerabilities in IIoT devices and systems. During the undertaking of the research and the preparation of the architecture, threats, and potential cyber-attack vectors on IIoT have been identified and presented based on experience in Figure 2. IIoT attack surface and potential entry points-from further investigation and looking deeper into the details of common cyber-attack vectors at the IIoT, we will have a more enlightening view. Figure 2 provides a representation of the IIoT attack surface, including association with communication protocol, port, industry sector involved, and attack surface intentions. The attack surface in IIoT refers to several opportunities for potential weaknesses and entry points, which can be targeted by attackers to compromise the security and integrity of IIoT systems. From these attack surfaces identified as the possibility of malicious actors' entry into the infrastructure of the IIoT, the impact will be lossy and high because each one presents a risk for serious cyber-attacks. Let's see the case of IIoT attack surface from Figure 2: "Open and Unnecessary Ports" mentions the risk of open and accessible ports in IIoT devices, which will potentially lead to attacks and unauthorized access to devices and more widely.



Industrial IoT (IIoT) Attack Surface	IIoT Communication Protocols and Ports used/ Industry sector/ Attack surface intention
Insecure Device Firmware	• MQTT (Port 1883), OPC UA (Port 4840) Manufacturing. Exploiting vulnerabilities in device firmware to gain unauthorized access.
Weak Authentication/Authorization	• DDS (Port 7401), Modbus (Port 502) Industrial Automation. Unauthorized access and control of industrial systems and devices.
Lack of Data Encryption	• LoRaWAN (Port 1700), BLE (Bluetooth) Agriculture, Healthcare. Interception and manipulation of sensitive data transmitted over the network.
Vulnerable Network Infrastructure	• Wi-Fi (Port 80, 443) Various Sectors. Targeting weaknesses in Wi-Fi networks to gain access to IIoT devices.
Insufficient Device Management	• MQTT (Port 1883), OPC UA (Port 4840) Energy, Smart Cities. Exploiting poor device management practices for unauthorized actions.
Inadequate Security Monitoring	• DDS (Port 7401), Modbus (Port 502) Aerospace, Defense. Exploiting the lack of real-time monitoring and response capabilities.
Lack of Physical Security	• Wi-Fi (Port 80, 443), BLE (Bluetooth) Transportation, Retail. Physical tampering or theft of IIoT devices.
Open and Unnecessary Ports	• All IIoT Protocols and Associated Ports All Sectors. Exploiting open ports to gain unauthorized access and launch attacks.

Figure 2. Industrial IoT attack surface

A summary of the potential attack surface at the IIoT device level is presented in Figure 2 where different attack surfaces are related to communication protocols (e.g. ports), industry sector, and attack surface impact. These are important because by identifying which are the most common attack surfaces, you can detect vulnerabilities that the attack can exploit and find ways to defend against them. Common cyber-attack vectors that present possible entry points include unauthorized access, firmware exploitation, device theft, malicious code injection, ransomware, sniffer, and DoS flooding the network. However, the cyber security challenge remains, while common cyber-attack vectors can exploit vulnerabilities within the system and get unauthorized access. By addressing these cyber-attack vectors through the proposed model, the industry can advance the level of cyber security for their IIoT systems. This proposed model combines functions and provides recommendations in the form of countermeasures, offering comprehensive protection against cyber threats. The countermeasures recommended by the proposed model include level, technical, operational, and policy security controls. The perception and addressing of such identified risks or threats highlight the need to develop robust security countermeasures and use effective risk management strategies in industrial environments.

So, practically, initiating cyber-attacks by the attacker follows a method and path to success. These methods and paths are interrelated and in cyber security, they are known as hacking methodology or penetration testing process. First, the attacker identifies the attack surface of the target, and then the attack vector that corresponds to that attack surface is used to exploit a vulnerability within that surface [1], [6]. Further, after exploiting the vulnerability on that surface, specific cyber-attacks related to that attack vector are launched. The attack vectors are methods and techniques used by the attacker to exploit vulnerabilities, that is, verification of whether that vulnerability exists or not. Meanwhile, cyber-attacks are specified as actions taken by the attacker to exploit the vulnerabilities and achieve the malicious objective of the attack.

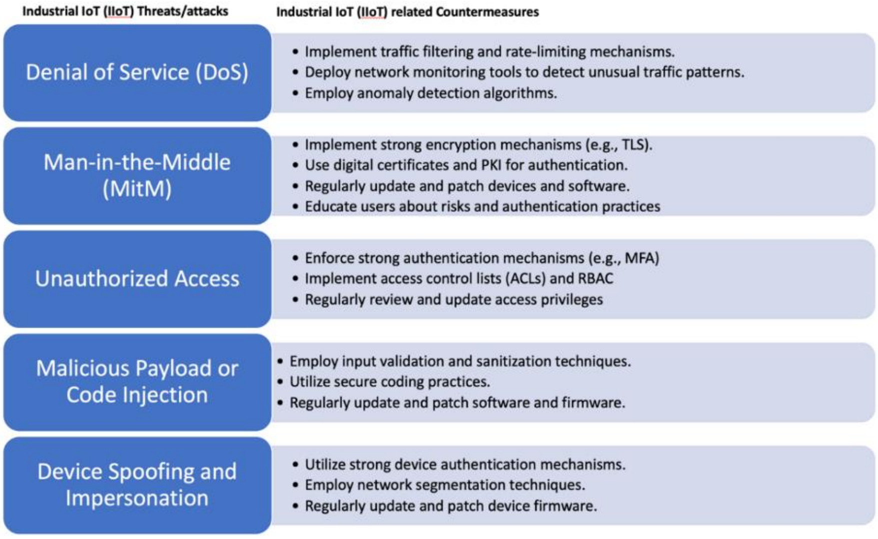
Known IIoT security threats to the countermeasures in this part of the section, we have identified several known security threats, because of the existence of vulnerabilities in IIoT devices, as presented previously. We also present countermeasures regarding threats and potential vulnerabilities of an IIoT device that can be exploited, a scheme is also presented in Figure 3. Communications of IIoT practically the protocols used are important, in the face of cyber-attacks [7], [8]. Threats to IIoT protocols can vary based on the specific protocol used, and their implementation (security controls) [9], [10].

DoS one of the most well-known types of threats and attacks is the DoS attack. Such an attack occurs whenever the attacker tries to flood the server or the IIoT device with traffic packets, in this way disrupting or crashing it, and putting it out of service [11]. DoS attacks have a great impact on the technical aspects of IIoT systems. Then, the sensitivity and the points where it can have an impact depending on the nature and scale of the attack, but also on the IIoT infrastructure targeted. The technical impacts of the DoS attack on IIoT systems include system availability, network congestion, device overload, exhaustion of resources, and data integrity.

Man-in-the-Middle (MitM)-another IIoT security threat and attack is MitM attacks. MitM attacks on IIoT systems can compromise communication and data sharing security and integrity within the IIoT infrastructure [12], [13]. The most common ways of undertaking this attack and falling prey are two, one is through phishing. For example, the attacker sends phishing emails and asks you to provide credentials in a certain form because as this email says they are necessary for your organization and work. If you provide those credentials, then the attacker can access your account and intercept your communications with everyone. A second way of MitM attack is through access to public wireless networks, where the level of security does not exist at all. The moment the attacker gets access to the router of that network, an attacker can intercept and receive all the data that is transmitted [14].

Unauthorized access - an unauthorized access attack on IIoT has an impact and reaches data breach, unauthorized control, and compromises the authentication mechanism. The best defense against these types of attacks is through responding at any time, maintaining the security system, and securing the data storage where it is stored [15]. Malicious payload or code injection - different types of attacks can be carried out such as malicious payload code injection, including SQL injection (SQLi), Cross-Site Scripting (XSS), remote code execution (RCE), and code injection in IoT Firmware. For example, a malicious payload occurs when the attacker sends an infected payload to the device or server that IIoT communicates, which can lead to data corruption and theft. By sending this malicious payload, and by triggering it inside the targeted infrastructure, it enables the attacker to receive the data, in a way opening the connection with the target in this case through the code injection attack [16]. However, this attack can only be carried out when there are security weaknesses in the software, and malicious code can be executed.

Device spoofing and impersonation - for example, device spoofing and impersonation occur when an attacker impersonates a legitimate IIoT device or their nodes to gain unauthorized access to networks, manipulate data, or launch other attacks. Now that we covered IIoT threats and potential vulnerabilities that can be exploited above, we can mention countermeasures and prevention of attacks. We show various known IIoT threat attacks, as well as the methods that the attacks use. Figure 3 is broken down, and specific examples of attacks are provided along with countermeasures that can be used further to secure IIoT devices.



Industrial IoT (IIoT) Threats/attacks	Industrial IoT (IIoT) related Countermeasures
Denial of Service (DoS)	• Implement traffic filtering and rate-limiting mechanisms. • Deploy network monitoring tools to detect unusual traffic patterns. • Employ anomaly detection algorithms.
Man-in-the-Middle (MitM)	• Implement strong encryption mechanisms (e.g., TLS). • Use digital certificates and PKI for authentication. • Regularly update and patch devices and software. • Educate users about risks and authentication practices
Unauthorized Access	• Enforce strong authentication mechanisms (e.g., MFA) • Implement access control lists (ACLs) and RBAC • Regularly review and update access privileges
Malicious Payload or Code Injection	• Employ input validation and sanitization techniques. • Utilize secure coding practices. • Regularly update and patch software and firmware.
Device Spoofing and Impersonation	• Utilize strong device authentication mechanisms. • Employ network segmentation techniques. • Regularly update and patch device firmware.

Figure 3. Known industrial IoT security threats to the countermeasures

This paper is organized into sections, the first section provides industry research information, previous research work on IIoT architecture, attack surface, and potential entry points, and types of threats to IIoT countermeasures. The second section used methodology describes the methods utilized to show the production and integration of such an approach model proposal. Section three is a detailed discussion of the proposed model, its main functions, model integration, and workflow overview. Section four results and discussions provide a narrative that readers understand the meaning of the findings and proposal. Lastly, the section conclusion provides a comprehensive model proposal, addresses the contribution of the research, and discusses potential applications of the proposed model, and future research directions.

2. METHOD

This section introduces the methodology employed in applied research focus in designing our proposed cyber security model for IIoT systems. The methodology lays out the structured approach taken to address the research objectives. The main objective of our research is to design a cyber security model that enhances the security, stability, and protection of IIoT systems. This proposed model aims to address existing cyber security challenges and vulnerabilities in IIoT environments. This includes identifying the security posture and threats, categorizing threats and vulnerabilities into impact levels, providing countermeasures, and evaluating countermeasures from a cost-benefit perspective. In our previous research work [3], [17], we conducted a comprehensive literature review to collect existing research work, solutions, and insights related to cyber security in IIoT. The previous work analysis on the current solutions has indicated the opportunities to work on the design of the model which advances the level of security in IIoT. The literature review helped identify the current gaps and limitations of the field, providing a basis for our research. The findings [3], [17] show us that IIoT is critical with the current level of cyber security during its operation processing, storing, and transmitting data. Based on our methodology in applied research, we develop the proposed cyber security model for IIoT. The methodology surrounds a structured approach, including a literature review, experienced expertise, and model enhancement.

Literature review - a thorough literature review [3], [17] was handled to identify existing research, gaps, and insights associated with cyber security in IIoT. Relevant academic journals, conference proceedings, industry reports, and our field expertise were analyzed to understand current practices, challenges, and emerging trends in IIoT security. Experienced expertise – our team’s field expertise in cyber security, IIoT systems, cryptography, and industrial automation was advised to collect domain-distinct knowledge and insights. Among us as experts, meetings and intensive work were handled to confirm the findings from the literature review, identify gaps in actual paths, and collect input on the design and development of the proposed model.

Model development - grounded on the findings from the literature review and expert advice, an introductory abstract structure for the cyber security model came into existence. This structure defined the main functions of the proposed model, including penetration testing, threat assessment, security Cost-Benefit Analysis approach (CBA), and countermeasure recommendation. Model refinement – the introductory model goes through repetitive refinement via feedback rounds with experts and understanding real-world examples situations. Feedbacks were integrated to advance the model’s feasibility.

Integration of standards and frameworks – over the model development operation, settled standards and frameworks were considered references to assure alignment with industry best practices and requirements. The standards supplied guidance on security controls, risk management, and compliance related to the IIoT industry including ISO/IEC 27001, 27002, NIST cyber security framework, and IEC 62443. Our research is based on an innovative model and incorporates as we explained settled principles and models of the field of Cyber Security and IIoT. It also integrates functions including penetration testing, risk assessment, and assurance of effective countermeasures based on a CBA.

2.1. Experimental setup

A thorough literature review was handled to identify, existing research, gaps, and directions in cyber security for IIoT systems [3]. Relative academic journals, conference proceedings, industry reports, and our field expertise were analyzed as input for the design of the model. Penetration testing process – the penetration testing process was utilized to evaluate the security posture of IIoT systems [17]. This included simulated cyber attacks to identify vulnerabilities and attack surfaces in the system's defenses, proper to OWASP methodology. Threat assessment methods – to evaluate the impact of identified threats threat assessment methods were utilized based on the OWASP risk assessment [17]. Threats were grouped based on the risk to IIoT systems, coaching the prioritization of the attacks, and countermeasures. Security CBA – a cost-benefit analysis was managed to provide organizations with the too precious solution to protect and enhance the security posture of IIoT systems. This included assessing from the perspective of the cost related to countermeasures upon benefits of mitigating identified threats and cyber-attacks. Countermeasure generation process – went through providing effective recommendation countermeasures based on reference method common vulnerabilities and exposures (CVE) and model references. The process utilized input insights from penetration testing, threat assessment, and CBA to provide proper countermeasures. Here tools like Python scripts were employed to automate the process of getting feeds to particular threats and generate countermeasures [17].

2.2. Data analysis

Findings from the penetration testing process were examined to find vulnerabilities and attack vectors in IIoT systems. These findings enlightened the generation of countermeasures to mitigate identified vulnerabilities. Threat assessment results were analyzed to group threats based on their impact level according to OWASP risk assessment methodology. This analysis supported prioritizing the threats and vulnerabilities mitigation into levels of risk. The cost-benefit analysis involved evaluation by financial indications of implementing countermeasures. This analysis aided stakeholders make informed decisions relating to resource allocation for cyber security actions. Judgments related to the inclusion and exclusion of data were made based on the severity and impact of threats, and relevance to the research objectives. Through cyber security practice exists a process of exploitation of identified vulnerabilities by bringing out the real potential cyber-attacks.

3. PROPOSED MODEL

In this section, we present in detail the proposed model for enhancing cyber security for IIoT. When we evaluate the security posture of IIoT systems, it is necessary to use any penetration testing methodology and tools, as well as the definition of attacks, and the procedure of penetration testing. A structured and proactive approach to developing such security tests is to follow the development of the four-step process and define the security testing steps for each. The following part of the section shows the proposed model functions and security testing actions up to the development of the process in general as supported by the references of established standards and frameworks.

The initial phase consists of planning the assessment of security posture (penetration testing), while the next phase collects the findings and organizes (findings, data sorting, and categorization operation), the continuation with the security analysis also from the aspect of cost-benefit (security analysis), finishing (report delivery) and documentation of recommended countermeasures. While this proactive approach for its purpose needs to use software and tools, the process is similar for all sectors of the industry (for example, the process of setting up cyber security for the industrial systems [18], [19]). For the model to provide results in the provision of cyber security for IIoT, we focus on the design, implementation, and recommendation of countermeasures phase of the model and specify the four main functions in more detail: i) penetration testing (attack testing); ii) threat assessment, and data categorization; iii) security cost-benefit analysis, and countermeasure generation; and iv) cyber security countermeasure report. By integrating these functionalities, the model enables stakeholders to effectively identify and address vulnerabilities, enhance the security posture of systems and networks, and allocate resources efficiently for risk mitigation and countermeasures implementation.

3.1. Penetration testing

Penetration testing, as we know ethical hacking, is a systematic structured process for testing computer systems to identify threats and potential vulnerabilities. These security tests can be conducted either way from outside and from inside the infrastructure to ensure that all attack possibilities are covered. The objective of each penetration test is to establish guidelines and recommendations for fixes in addressing the findings. Appropriate planning is very important in defining the purpose, and objectives of testing the target system, network, device, or application. The planning includes contractual measures that usually consist of authorization or contracts that define the scope of the penetration test, the schedule of conducting the test, the human resources involved, and the reporting. For the penetration testing process, different ways can be used, but two are the main ones also based on the information that the attacker may have.

Black box testing: only have the initial information of the target, or we have no information at all. White box testing: most of the information is known to the attacker. More, information about the system is available. Penetration Testing phases are the steps that the test must go through and can be presented as follows [20], [21]:

- Reconnaissance and information gathering: the initial phase, collecting information about the target system, networks, device, or application. All the information found is used in the next phase of testing.
- Scanning: at this stage, tools are used to further test in depth to potentially identify target vulnerabilities.
- Exploitation and gaining access: in this phase, the exploitation methods and techniques of the target are utilized, by using all the information gathered from the other phases.
- Maintaining access: for an attacker, it is important to stay in continuous connection with the target, because in that way attacker collects more data about him.
- Covering tracks: this phase is known for clearing any traces in the logs so that the unauthorized access of the attacker remains anonymous.

Required input for penetration testing process. To begin this testing process, we need initial information that determines the start of the process. It also depends on the way of testing (black-box or white-box testing), but the input is necessary for the initiation phases of penetration testing. Required input includes these and not only depending on the penetration testing scope, targets: IP addresses, hostname, network data, web links, and software versions or operating systems.

3.2. Threat assessment and data categorization

In this function operation, after the execution of the penetration testing process, the function of the model takes over the task of analyzing and organizing the findings. The findings introduce the vulnerabilities and potential entry points of cyber-attacks. It means that the attack surface for the target has been recognized, and potentially the attack vectors have been verified in the exploitation phase of penetration testing. Attack vectors represent vulnerabilities in the tested system, network, device, or application. Each attack vector is related to a cyber-attack in the background that can occur if countermeasures are not determined. In addition, recognized reference standards, frameworks, cyber security controls, methodologies, and guidelines of the model were also consulted. The analysis and evaluation of the findings determine their category, according to their impact on such cyber-attacks.

3.3. Security cost-benefit analysis and countermeasure generation

In security analysis based on the findings and model references standards and frameworks, countermeasures are generated. Information is studied to provide recommendations for countermeasures that would minimize or eliminate vulnerabilities. At this point, tools and scripts can be used to automate actions, especially about obtaining additional information about fixes of vulnerabilities. In this research paper, Python scripts are used to automate the knowledge acquisition of this additional information for each vulnerability at the model references. While the security analysis is being done, the model takes a general approach and produces a cost-benefit estimation forecast, for recommended countermeasures. Moreover, assessment of the risk, and cost-benefit for the recommended cyber security countermeasures to be implemented, be of use to organizations to have affordable solutions [22]. The proposed cyber security model for IIoT is built on the foundations of recognized standards and frameworks and adapted for the industry. The model references in our research include a wide range of recognized standards such as the [23] cybersecurity framework, ISO/IEC 27001, 27002, and IEC 62443, Cybersecurity and Infrastructure Security Agency (CISA), open IIoT, Forum of Incident Response and Security Teams (FIRST), ENISA Good Practices for IoT and smart infrastructures tool, the open web application security project (OWASP), open-source security testing methodology manual (OSSTMM), penetration testing execution standard (PTES), and open-source intelligence (OSINT). Based on the data of the model functions specific penetration testing process, the selection of these references is also made as an important attribute of the vulnerabilities identified. After the analysis of the data, the vulnerabilities of the model function penetration testing process [24], [25] and the assessment from the security aspect, and then sorting and grouping them into impact categories using the OWASP methodology [24], where the categories level are established of critical, high, medium, and low. In the next phase, knowledge acquisition [26]-[35] is conducted, taking the basic and complementary information of the vulnerabilities [36], [37], by generating the recommendations for cyber security countermeasures one by one. After the discovery of the countermeasures, data were regrouped by repeating successive iterations until the optimal recommendations were found for associated vulnerabilities. By continuously evaluating the cost-benefit analysis for recommendations countermeasures [38], the final checklist is reached that supports the decision-makers at the organizations for the most possible and cost-effective solutions.

3.4. Cyber security countermeasure report

Once the comprehensive analysis cyber security state of the IIoT system has been conducted, including the identification of vulnerabilities associated with risk threats, grouping and categorization, generation of countermeasures based on model references, as well as their cost-benefit evaluation. At this time, the next function delivers the final report documenting the findings. This report serves as a means of communication, offering the organization and parties valuable insights into the security posture of the IIoT system and recommending actions for mitigating identified vulnerabilities. Complementary, the report includes the evaluation of the cost-benefit analysis to see the financial impacts of implementing the recommended cyber security countermeasures.

3.5. Model integration and workflow

In the section above we explained in detail the proposed model functions, highlighting its key components and their interconnections. We elaborated on specific steps involved in integrating the different security measures within the proposed model. The successful implementation of sustainable cyber security measures against threats and attacks in IIoT environments necessarily requires the integration of multiple functions to have an effective defense strategy. In this section, we present the model that perfectly integrates the functions of penetration testing, threat assessment, data categorization, security cost-benefit analysis, and countermeasure generation. The purpose and objective of the research, the integration of these important functions is to provide a proactive approach to enhance and reinforce the level of cyber security in IIoT systems. This comprehensive approach entitles industrial organizations to detect and mitigate potential vulnerabilities effectively, strengthen security posture, and defend their critical infrastructure. Figure 4 presents the workflow overview of a proposed model of cyber security for IIoT including the sequence of operations, information flows, and decision points that occurred. The visual presentation of the model diagram, workflow steps, and interconnections is made using the business process model and notation (BPMN).

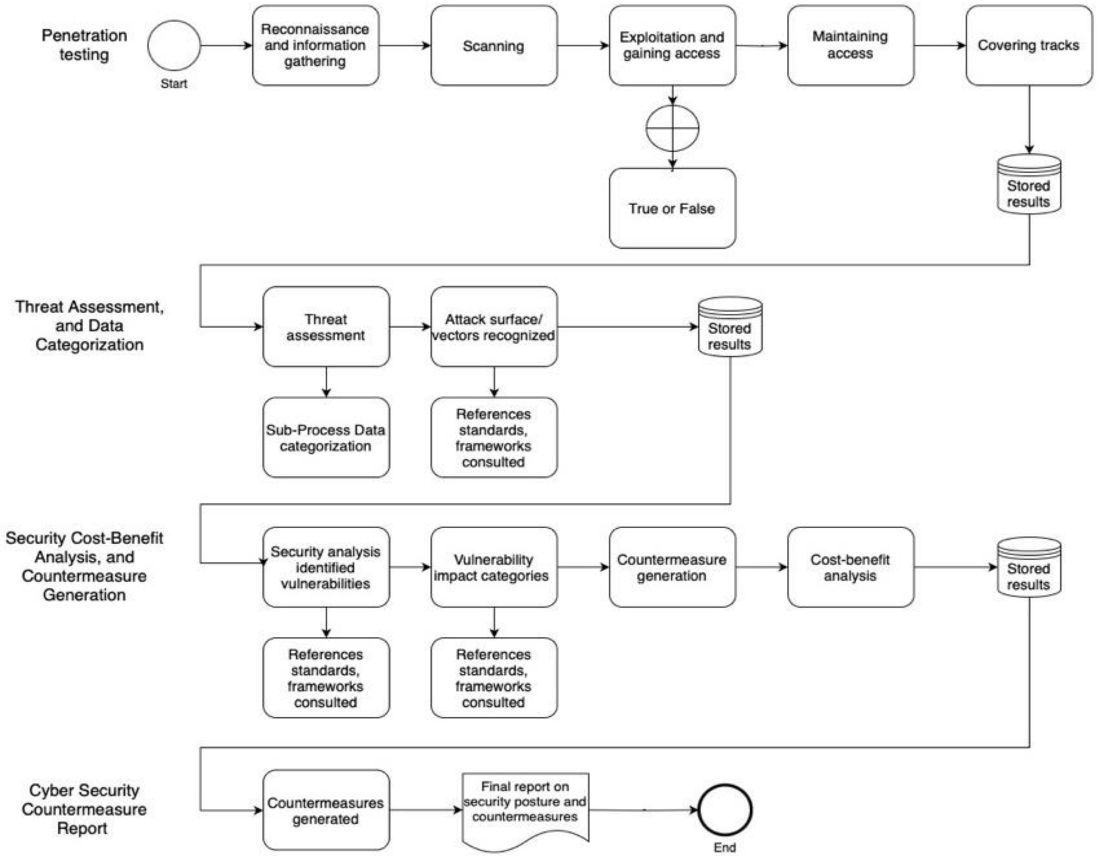

Penetration testing
Start
Reconnaissance and information gathering
Scanning
Exploitation and gaining access
Maintaining access
Covering tracks
True or False
Stored results
Threat Assessment, and Data Categorization
Threat assessment
Attack surface/ vectors recognized
Stored results
Sub-Process Data categorization
References standards, frameworks consulted
Security Cost-Benefit Analysis, and Countermeasure Generation
Security analysis identified vulnerabilities
Vulnerability impact categories
Countermeasure generation
Cost-benefit analysis
Stored results
References standards, frameworks consulted
References standards, frameworks consulted
Cyber Security Countermeasure Report
Countermeasures generated
Final report on security posture and countermeasures
End

Figure 4. Workflow steps overview of the proposed model

4. RESULTS AND DISCUSSION

The advent of IIoT has changed industrial operations, advancing efficiency and quality. However, this technological enhancement has also accompanied an increase in cyber-attacks targeting IIoT systems. The research addresses these challenges by proposing a cyber security model for IIoT. Previous studies have explored the impact of common cyber threats targeting IIoT systems, such as malicious code injection, DoS attacks, and unauthorized access. Our study found that traditional cyber security measures have shown a lack in mitigating these threats to IIoT systems. Traditional security measures like the CIA triad and antivirus solutions demonstrate lacking addressing the advanced modern cyber-attacks. The proposed solutions entail ML algorithms, blockchain integration, and intelligent DoS detection frameworks. Nevertheless, challenges exist in implementing these solutions effectively, and a need beyond research to design proactive cyber security approaches specific to IIoT. Evidence from the research study is outlined in Table 1 provides insights into the major findings discussed earlier.

Our findings underline the criticality of cyber security in protecting IIoT systems against growing cyber threats. However, the proposed cyber security model provides a proactive approach by integrating functions such as penetration testing, threat assessment, security cost-benefit analysis, and countermeasure recommendations. Benefiting standards and frameworks like ISO/IEC 27001, NIST cybersecurity framework, and IEC 62443, the model delivers organizations with a structured model for advancing the security posture of IIoT systems. This proactive approach empowers stakeholders to identify vulnerabilities, prioritize threats, and assign resources efficiently for risk mitigation. Our study findings have indications for policy drafting in the field of cyber security for IIoT. By emphasizing the need for enhanced cyber security countermeasures and proactive threat mitigation, the study advises policymakers on the urgent need to sort cyber security investments and regulations in industrial sectors. The proposed cyber security model has applicable indications for advancing the resilience of IIoT systems against cyber threats. By incorporating advanced security measures and benefiting from emerging technologies like ML and blockchain, organizations can maintain their defenses and mitigate potential risks. However, the model's limitations and possible challenges in implementation need further exploration. Future research includes advance and validation of the proposed model through practical implementations and case studies. Nevertheless, the success of the model may differ based on the specific characteristics and configurations of different industrial systems. Furthermore, continuing research is needed to handle emerging cyber threats and vulnerabilities specific to IIoT applications, and secure continuous advances in cyber security practices. Our study highlights the criticality of cyber security in safeguarding IIoT systems against evolving cyber threats. The proposed cyber security model offers practical insights for policymakers and industry stakeholders, emphasizing the need for advanced cyber security countermeasures and proactive threat mitigation strategies. Collaboration, partnerships, and knowledge sharing between industry stakeholders, researchers, and policymakers are vital to designing thorough strategies for the protection of IIoT systems and critical infrastructure against cyber threats.

Table 1. The insights into the major findings

Findings	Description
Common cyber security threats in IIoT	Identified vulnerabilities include lack of privacy, common cyber-attacks (malicious code, DoS), and emerging threats targeting weak security areas.
IIoT attack surfaces and entry points	Attack surfaces include open ports, communication protocols, and industry-specific vulnerabilities.
Known IIoT security threats and countermeasures	Threats include DoS, MiTM attacks, unauthorized access, and malicious code injection. Countermeasures involve access control, encryption, and network monitoring.

5. CONCLUSION

In this paper, we presented a comprehensive model proposal of cyber security for the IIoT. Therefore, our model provides a proactive approach to advance cyber security resilience by integrating functions such as penetration testing, threat assessment, data categorization, security cost-benefit analysis, and cyber security countermeasure recommendations. To address security challenges, our proposed model provides a proactive approach integrated with joint functions to enhance cyber security resilience in IIoT systems. Through these functions, stakeholders can assess the security posture of IIoT, identify vulnerabilities, prioritize risks, and recommend countermeasures guided by cost-benefit analysis. By receiving information from penetration testing and threat assessment, we can quickly find vulnerabilities and potential attack vectors, and support stakeholders for the implementation of protective countermeasures. Data categorization ensures the effective organization of data related to security and support for prioritizing appropriate actions based on the impact of risk. The security cost-benefit analysis function specifies the financial cost implications of implementing countermeasures, helping stakeholders make informed decisions about the necessary resources. The last is the generation of countermeasures that prepare actions for security measures to address the weaknesses found, according to the organization's strategic goals and risk tolerance.

Looking forward, we understand the significance of beyond research and refinement of our model. Future works will focus on building the model utilizing ML algorithms to advance the model's capabilities, testing the model in simulated IIoT infrastructure, or at any University Laboratory; and evaluating its performance through ML metrics. Furthermore, we aim to prototype an enhanced model of cyber security for IIoT that corresponds with organizational goals and risk tolerance. By handling these plans, we aim to contribute to the ongoing efforts to protect IIoT systems and fortify cyber security resilience in industrial settings.

REFERENCES

[1] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial IoT devices," *ACM Transactions on Internet Technology*, vol. 20, no. 2, pp. 1–24, May 2020, doi: 10.1145/3379542.

[2] J. W. Jang, S. Kwon, S. J. Kim, J. Seo, J. Oh, and K. H. Lee, "Cybersecurity framework for IIoT-based power system connected to microgrid," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 5, pp. 2221–2235, May 2020, doi: 10.3837/tiis.2020.05.020.

[3] A. Buja, M. Apostolova, A. Luma, and Y. Januzaj, "Cyber security standards for the industrial internet of things (IIoT)– a systematic review," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Jun. 2022, pp. 1–6, doi: 10.1109/HORA55278.2022.9799870.

[4] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: internet of threats? a survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[5] C. Pettey, "Navigating the security landscape in the IoT era," *Gartner*, 2016. https://www.gartner.com/smarterwithgartner/navigating-the-security-landscape-in-the-iot-era.

[6] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network," *Internet of Things*, vol. 9, p. 100162, Mar. 2020, doi: 10.1016/j.iot.2020.100162.

[7] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for IoT security," in *2014 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2014, pp. 183–188, doi: 10.1109/ICCNC.2014.6785328.

[8] S. H. Mekala, Z. Baig, A. Anwar, and S. Zeadally, "Cybersecurity for industrial IoT (IIoT): threats, countermeasures, challenges and future directions," *Computer Communications*, vol. 208, pp. 294–320, Aug. 2023, doi: 10.1016/j.comcom.2023.06.020.

[9] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: A survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, Mar. 2021, doi: 10.3390/iot2010009.

[10] R. Ankele, S. Marksteiner, K. Nahrgang, and H. Vallant, "Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, Aug. 2019, pp. 1–8, doi: 10.1145/3339252.3341482.

[11] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino, and S. E. Quincozes, "Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4569–4578, Mar. 2021, doi: 10.1109/JIOT.2020.3028652.

[12] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua, and P. Haskell-Dowland, "Hybrid routing for man-in-the-middle (MITM) attack detection in IoT networks," in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2019, pp. 1–6, doi: 10.1109/ITNAC46935.2019.9077977.

[13] S. Pallavi and V. A. Narayanan, "An overview of practical attacks on BLE based IOT devices and their security," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Mar. 2019, pp. 694–698, doi: 10.1109/ICACCS.2019.8728448.

[14] R. E. Navas, H. Le Bouder, N. Cuppens, F. Cuppens, and G. Z. Papadopoulos, "Demo: do not trust your neighbors! a small iot platform illustrating a man-in-the-middle attack," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11104 LNCS, 2018, pp. 120–125.

[15] M. Jovic, E. Tijan, S. Aksentijevic, and D. Cisic, "An overview of security challenges of seaport IoT systems," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2019, pp. 1349–1354, doi: 10.23919/MIPRO.2019.8757206.

[16] H. A. Noman and O. M. F. Abu-Sharkh, "Code injection attacks in wireless-based internet of things (IoT): a comprehensive review and practical implementations," *Sensors*, vol. 23, no. 13, p. 6067, Jun. 2023, doi: 10.3390/s23136067.

[17] A. Buja, M. Apostolova, and A. Luma, "Enhancing cyber security in industrial internet of things systems: an experimental assessment," in *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, Jun. 2023, pp. 1–5, doi: 10.1109/MECO58584.2023.10155100.

[18] P. Zhu and J. P. Liyanage, "Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: a specific review of issues and challenges in safety instrumented systems," *European Journal for Security Research*, vol. 6, no. 2, pp. 125–149, Dec. 2021, doi: 10.1007/s41125-021-00076-2.

[19] J. Park, Y. Suh, and C. Park, "Implementation of cyber security for safety systems of nuclear facilities," *Progress in Nuclear Energy*, vol. 88, pp. 88–94, Apr. 2016, doi: 10.1016/j.pnucene.2015.12.009.

[20] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27–49, Feb. 2015, doi: 10.1007/s11416-014-0231-x.

[21] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, May 2018, pp. 1–7, doi: 10.1109/LISAT.2018.8378035.

[22] S. Kim and H. J. Lee, "Cost-benefit analysis of security investments: Methodology and case study," in *Lecture Notes in Computer Science*, vol. 3482, no. III, 2005, pp. 1239–1248.

[23] "Cybersecurity framework," *NIST*. [Online]. Available: https://www.nist.gov/cyberframework.

[24] "Attack surface analysis cheat sheet," *OWASP*. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html.

[25] J. Nordine, "OSINT framework," *osintframework.com*. [Online]. Available: https://osintframework.com/.

[26] "Cybersecurity framework," *Cybersecurity and Infrastructure Security Agency (CISA)*. [Online]. Available: https://www.cisa.gov/uscert/resources/cybersecurity-framework.

[27] "Using the cybersecurity framework," *Cybersecurity and Infrastructure Security Agency (CISA)*. [Online]. Available: https://www.cisa.gov/using-cybersecurity-framework.

[28] "FIRST standards," *Forum of Incident Response and Security Teams (FIRST)*. [Online]. Available: https://www.first.org/standards/.

[29] "Industrial communication networks - network and system security - part 1-1: terminology, concepts and models," *International Electrotechnical Commission (IEC)*, 2009. [Online]. Available: https://webstore.iec.ch/publication/7029.

[30] "Industrial communication networks - network and system security - part 2-1: establishing an industrial automation and control system security program," *International Electrotechnical Commission (IEC)*, 2018. [Online]. Available: https://www.singaporestandardseshop.sg/Product/SSPdtDetail/c8caa4d0-4af1-4fd6-a552-d14ff3ca59a6.

[31] "Security for industrial automation and control systems - part 2-4: security program requirements for IACS service providers," *International Electrotechnical Commission (IEC)*, 2017. [Online]. Available: https://webstore.iec.ch/publication/61335.

[32] "Understanding IEC 62443," *International Electrotechnical Commission (IEC)*, 2021. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443.

[33] "ISO/IEC 27005:2018," *www.iso27001security.com*, 2018. [Online]. Available: https://www.iso27001security.com/html/27005.html.

[34] "ISO/IEC 27001 information security management systems," *ISO*, 2022. [Online]. Available: https://www.iso.org/standard/27001.

[35] "ISO/IEC 27002:2022 information security, cybersecurity and privacy protection — information security controls," *ISO*, 2022. [Online]. Available: iso.org/standard/75652.html.

[36] "CVE DB," *MITRE*, 2023. [Online]. Available: https://cve.mitre.org/.

[37] "Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities," *CVE*. [Online]. Available: https://www.cve.org/.

[38] S. Papa, W. Casper, and T. Moore, "Securing wastewater facilities from accidental and intentional harm: a cost-benefit analysis," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 96–106, Jun. 2013, doi: 10.1016/j.ijcip.2013.05.002.

BIOGRAPHIES OF AUTHORS

Atdhe Buja Ph.D. is an EC-Council Instructor. He holds an M.Sc. degree in Computer Science and is a certified professional in the industry as a Certified EC-Council Instructor (CEI), CEH, MCITP, OCA, and CIO. His research areas are cybersecurity for IoT, IIoT, WSN, and digital forensics. He got a "Patent of the Computer program for WSN IoT nodes Simulation on Sinkhole attack identification" verify link https://copyright.kazpatent.kz/?!.iD=PMZU. He is the director of the ICT Academy Research and Innovation Lab, a member of the International Science Complex in Astana, and a NIST GCTC member. He is the founder of ICT Academy which is a Cyber Security-based company and their innovative services received appreciation at national and international levels. Link to resume at: website https://www.atdheb.com or LinkedIn: https://www.linkedin.com/in/atdhebuja/. He can be contacted at email: atdhe.buja@hotmail.com.

Assoc. Prof. Dr. Marika Apostolova Docent at South East European University. Experienced Docent with a demonstrated history of working in higher education at the Faculty of Contemporary Sciences and Technologies (CST) at South East European University (SEEU) in Macedonia. During her teaching experience, she has taught courses from the area of data structures and algorithms, C++ programming, object-oriented programming, web programming, software engineering, strategic information technology project management, interactive system design, software project management, and Microsoft IT courses. She is active in research and was acting as project manager-coordinator of the DISCO - Erasmus+ KA201 international project. She was also the coordinator of Integrated study programs that were part of a project between the German Federal Government of Development Cooperation and SEEU. Link to resume at: https://www.seeu.edu.mk/en/~m.apostolova. She can be contacted at email: m.apostolova@seeu.edu.mk.

Prof. Dr. Artan Luma full Professor at South East European University (SEEU). He was the Project Manager Youth Resource Center - ICan, Gostivar, North Macedonia. A long experience in academic institutions including Associate Professor; Faculty of Computer Science and Engineering at UBT, Iliria, SEEU, and Deputy Director of the e-Learning Center. Link to resume at: https://www.seeu.edu.mk/en/~a.luma. He can be contacted at email: a.luma@seeu.edu.mk.