12-12-2021

Process business modeling of emerging security threats with BPMN extension

Tomasz Krym
Lodz University of Technology

Lukasz Chomątek
Lodz University of Technology

Aneta Poniszewska-Marańda
aneta.poniszewska-maranda@p.lodz.pl

Process business modelling of emerging security threats with BPMN extension

Tomasz Krym
Institute of Information Technology, Lodz University of Technology,
Lodz, Poland, tomasz.krym@dokt.p.lodz.pl

Łukasz Chomątek
Institute of Information Technology, Lodz University of Technology,
Lodz, Poland, lukasz.chomatek@p.lodz.pl

Aneta Poniszewska-Marańda [1]
Institute of Information Technology, Lodz University of Technology,
Lodz, Poland, aneta.poniszewska-maranda@p.lodz.pl

ABSTRACT

Effective and rational management of a company cannot take place without the use of information technologies. Additionally, according to specific security requirements to protect the IT system against different threats, the development of a security system is significant for the companies and their clients and satisfactory common cooperation. The BPMN (Business Process Model and Notation) can be used for this purpose; however, the basic version of BPMN and its current extensions do not support the service of security threats. For this reason, we propose to extend the BPMN to be possible to model the chosen security issues coming from company business processes. The paper deals with the selected aspects of security requirements modelling in terms of emerging threats on the example of existing extensions of business process modelling language and the proposition of BPMN extension for chosen security issues together with the definition of information security policy.

Keywords: software modelling, business process, BPMN (Business Process Model and Notation), information systems security, security policy.

[1] Corresponding author. aneta.poniszewska-maranda@p.lodz.pl +48 42 631 27 96

INTRODUCTION

Nowadays, effective and rational management of a company or enterprise cannot occur without the use of information technologies. Single computers and applications installed on them are no longer sufficient. Computers and applications are connected with each other into a uniform computer network, the resources used by many users simultaneously. Thanks to this, it is possible that the data entered by one user is immediately made available to other authorized persons. In such a situation, it becomes natural to need an appropriate development of a security system, according to specific requirements, to protect the IT system against threats from inside a given company and its environment. The primary purpose of ensuring data protection is to reduce this type of risk to an acceptable level from the point of view of the proper functioning of the company. What is needed is a **"**financial compromise**"** between the price to be paid for ensuring an appropriate security level in the company and the cost of, for example, data loss caused by the lack or malfunctioning of any security system service.

The latest works of the field of cybersecurity indicate new threats related to the development of technology: based on deepfake – video call, voice call with a person impersonating a person having access or decision-making rights; attack on AI learning data – replacing learning data for a specific purpose, e.g. downplaying selected threats or incorrect answers in certain situations; interception of data in cloud computing – both for entire virtual machines in the IaaS (Infrastructure as a Service) model, as well as data necessary for applications – after the attacker breaks security protections at the application level,

ransomware attacks – carried out using the tools that track user activities and using various phishing techniques; theft of sensitive data for identity fabrication.

Thus, it can be seen that due to the emergence of new types of threats, they should be included in the applied security policies, in particular in the business processes. Of course, we are talking about already existing processes as well as processes under development (elicitation).

A business process can be defined as a set of tasks intended to deliver a product or service to a customer (Lindsay et al. 2003). The above activities should be coordinated and standardized within the company. As a result, processes can be *reusable*, which reduces the costs related to Business Process Management (OMG 2013, Chang 2016). Such processes can be classified according to their features: processes related to proper production or production coordination, processes performed by human or machine, processes triggered by internal or external factors (Chang 2016). Due to the variety of business processes, many works related to business process management have been produced, such as (Chang 2016, Dumas et al. 2013, Jeston and Nelis 2014, Kumar 2018, Tipton 2019). All these works indicate the necessity to present the business process in the form of a model, while the works such as (Kumar 2018; Tipton, 2019) focuses on security issues.

This paper analyses the current state-of-the-art in the aspects of modelling the security aspects and procedures on the example of existing extensions of business process modelling language BMPN2 (Business Process Model and Notation, version 2). Next, the proposition of BPMN extension for chosen security issues, together with the definition of information security policy is given. The proposition to extend the BPMN was made because the current extensions of BPMN do not support handling security treats.

SECURITY IN BUSINESS PROCESSES

The following aspects are taken into account in the security of business processes (Argyropoulos et al. 2019): Authentication, Authorization, Confidentiality, Integrity,

Availability. It should be noted that the implementation of individual aspects related to security is the research subject of security mechanisms in specific cases. It is also evident that companies do not provide detailed information about the security mechanisms and tools they have due to attackers' possibility of using this knowledge. Examples of possibilities to ensure the mentioned above security aspects and their meaning are presented in Table 1.

Table 1. Realization and Implementation Methods for Security Purposes

Security purpose	Realization and implementation methods
Authentication – verification of credentials of a subject executing the *activity* with the use of security mechanisms.	• logging using the login and password • two-factor authentication (*2FA*) (Acemyan et al. 2018) • use of blockchain technology (Hammi et al. 2018) • mechanisms using biometrics (Barni et al. 2019)
Authorization – restricts access to specific resources based on certain rules. The possibility to perform the activity depends on the permissions held by the process participant.	• role (Ahn and Hu 2007) • access control list (Ma et al. 2019) • attribute-based access control (Ding et al. 2019) • blockchain (Ma et al. 2019, Thwin and Vasupongayya, 2019)
Confidentiality – the property of data object that restricts an access to this object only to process participants who have the appropriate authorization.	• encryption (Liang et al. 2019) (Puthal et al. 2017) • techniques dedicated to the cloud (Thillaiarasu and ChenthurPandian 2019) (Tchernykh et al. 2019)
Integrity – confidence that the data is protected against unintentional modification in the process.	• blockchain (Liu et al. 2017) • remote verification (Ateniese et al. 2007)
Availability – it should be possible to perform an activity on any request.	• resource placement (Do and Kim 2019) • cloud platform (Pitchai et al. 2019) • virtualization platform (Vayghan et al. 2019)

The comparison presented in Table 1 shows that each of the above-mentioned security aspects can be achieved in many ways. The method selection to ensure security depends on the

implemented technologies, but it is not the subject of this paper. However, it was intended to indicate that the information concerning the details of the implementation of these security aspects should be reflected in the process model. For example, two-factor authentication often requires two different devices to gain access to the system. Other accessibility methods require additional software involved in the business process, such as backing up the documents.

BPMN AND ITS SECURITY EXTENSIONS

BMPN is an international standard in the field of business process modelling. This standard was created to ensure the portability of process definitions, which allows transferring process definitions between different suppliers' environments. It is noting that BPMN generally supports only those elements that occur in business processes.

BPMN Syntax and Semantics

The components of the BPMN diagram belong to the following basic categories: *Object flows* – define the behaviors in business processes. This category includes Events, Activities and Gates. *Data* – objects (*Data Objects*), inputs, outputs and datastores. *Connections* (*Connecting Objects*) – illustrate the transition to the following process elements or sending the messages. In addition, they describe the associations or connections between information and Artifacts. *Locations of process execution* (*Pool*) – determines a business unit; track (*Lane*) – specifies a Process Participant inside the business unit. *Artefacts* – allow to include additional information about the Process. Standard artefacts in BPMN are group and text annotation.

Security Extensions for BPMN

In recent years, there have been several reviews works on security modelling with the use of extensions to the BPMN standard (Agostinelli et al. 2019, Gaidels et al. 2018, Zareen et al. 2020). Chronologically, the first extension of the BPMN notation was the work of Rodriguez

(Rodríguez et al. 2007), where the extension dealt with the process diagram and interfered with its essential elements. This work aimed to take into account the safety requirements already at the level of process design. The main threats concerned the detection of potential harm, data integrity, privacy and access control. A particular type of diagram, *Secure Business Process Diagram*, was introduced in the class hierarchy, which is stored as a property the list of requirements of *Security Requirements* class, related to the aspects mentioned above.

A different approach called Sec-BPMN2 is shown in (Salnitri et al. 2014), where a two-phase approach was introduced. In the first phase, annotations related to security threats (Privacy, Access Control, Integrity etc.) are superimposed on the business process, and then the assumptions are verified using the BPMN-Q language. This language allows checking the correctness of the prepared model at the conceptual level. Compared to the approach indicated in (Rodríguez et al. 2007), SecBPN2 has more elements related to access control (authentication and authorization are distinguished). Still, it does not include any elements related to the detected threat (Gaidels et al. 2018).

In works (Maines et al. 2015, Maines et al. 2016), a graphical representation of security issues in BPMN diagrams in the form of a third dimension was proposed. According to the authors, such a necessity results from the multitude of additional elements (such as in solution presented in (Salnitri et al. 2014)) and disturbs the legibility of the diagrams being prepared. The authors of (Maines et al. 2015) identified as many as 79 components of the proposed ontology arranged hierarchically on four levels. The highest level is general issues such as *Access Control, Privacy, Availability, Integrity, Attack/Harm Detection and Prevention, Accountability*. At the next level, there are more specific issues, such as authentication for *Access Control*. The third

level specifies a detailed issue, e.g. subjects that can be authenticated are indicated. The last level is the types of authentication for a specific subject.

The topic related to business process modelling is also the protection of personal data in accordance with the guidelines of the GDPR (General Data Protection Regulation). This issue is addressed in (Agostinelli et al. 2019). The conducted research showed the patterns on how to model: the procedure in the case of *personal data breaches*, granting consent to the processing of personal data, providing the right to access data, providing personal data to third parties (*Right of Portability*), request to stop (*withdraw*) the processing of personal data, *rectify* of personal data and the *right to be forgotten*. The presented patterns of solutions are compliant with the GDPR guidelines. However, the implementing company is responsible for the effectiveness of its implementation.

A careful analysis of the literature shows that the proposed approaches to modelling the safety-related aspects in BPMN diagrams are different from each other, and at the same time, none of the proposed approaches has become the leading one. In work (Rodríguez et al. 2007) the advantage is certainly the small number of elements added to the BPMN diagram. (Salnitri et al. 2014) introduced eight annotations concerning the activity. These annotations are marked with a distinctive colour. Each annotation can have a set of attributes that define the type of used security mechanisms, e.g. RBAC for authorization. The ability to describe the security details is a very positive aspect of this method. Each of the approaches presented above has some significant drawbacks in modelling the new security threats. In work (Rodríguez et al. 2007), all safety issues are related to the diagram and not to its individual elements, e.g. *Flow Objects*. It is a wrong assumption because there may be only single activities in the process that require

considering the security requirements. The division of *Security Requirements* into five categories where availability is lacking also raises doubts.

A certain inconsistency characterizes the ontology developed in (Maines et al. 2015). For example, at its third level, sometimes some subjects can use the selected security mechanism, while in other cases, the methods of security implementation (e.g. types of firewalls) are at the same level. The tree structure also causes some elements' redundancy, e.g. personnel appear in two places in this hierarchy. Another disadvantage of the prepared ontology is its incompleteness, especially a few years after its publication. There are already known authentication methods or data security than those shown in the diagram in (Maines et al. 2015).

PROPOSED EXTENSION OF BPMN LANGUAGE

This section presents the proposed extension of BPMN language that enables the inclusion of security issues in the business process model. The first subsection defines the Information Security Policy. Based on this definition, an object model was built (second subsection), enabling the security policy to be presented in the BPMN diagram. The method of implementing the built model into the BPMN structure is shown in the last subsection.

Definition of Information Security Policy

The Information Security Policy, ISP, will be called as the following octuplet: ISP = (S, U, H, P, BP, R, SP, L), where:

- *S* – system covered by the security policy,
- *U* – set of system users *S*,
- *H* – set of hardware components of *S* system, important from the point of view *ISP*,
- *P* – set of parameters describing users from the *U* set or hardware from the *H* set,

- *BP* – set of business processes carried out in the *S* system, for which it is important to meet the security requirements,
- *R* – set of security rules that govern user and hardware activities on the *S* system,
- *SP* – set of security procedures; single procedure consists of one or more rules from set *R*,
- *L* – set of security levels; each level in *L* consists of one or more procedures in *SP*.

This way of defining the security policy allows for the convenient definition of security procedures and assigning these procedures to security levels. It was also assumed that:

- Each parameter $p \in P$ has a unique name.
- Each user $u \in U$ and each hardware component $h \in H$ can have several parameters assigned. It was denoted the set of parameters of user *u* and set of parameters of hardware *h* by *P(u)* and *P(h)*, respectively.
- Any number of rules from the *R* set can be associated with each user *u* and each hardware component *h*.
- The rule $r \in R$ is defined by specifying acceptable values for the parameters of users or hardware components. The rule is assumed to be satisfied if all parameter values for users and hardware specified in the rule are in the set of acceptable values.
- The allowed values for parameter *p* in rule *r* can be specified as a set or a range.
- Each of the security routines $sp \in SP$ consists of any positive number of rules from the *R* set. It is, therefore, clear that one security procedure may involve different users and different hardware components. To complete the security procedure, users and hardware components must have parameter values specified in the rules.

- Security procedures are grouped into security levels. The purposefulness of building the security levels results from the fact that ensuring security of business process $bp \in BP$.

Model of Classes for Security Policy

The above set of assumptions can be presented in the form of a class diagram shown in Figure 1. The `Component` class shows the user or hardware component represented as its child classes `User` and `Hardware`, respectively. With the class `Component`, the set of parameters described by the `Parameter` class objects is related. The diagram highlights the `desiredValues` attribute, which shows the set of acceptable values for a user parameter or hardware element parameter in the condition (class `Condition`) checked in the rule (class `SecurityRule`). Security rules are part of security procedures (class `SecurityProcedure`) and procedures are part of security levels (class `SecurityLevel`).

It should be emphasized that the presented structure of classes does not impose restrictions on the number of security levels, the number of security procedures within a level or the number of rules within a single security procedure. Each condition in a security rule is associated with a single component (user or hardware component) and a set of expected parameter values for that component. It allows to state that the presented security policy model meets the assumptions from the beginning of this section.

Security Policy in BPMN Structure

Placing the security policy model shown in the section *Definition of Information Security Policy* requires the extension of the model known from the BPMN language specification (OMG, 2013). According to this specification, the process (class `Process`) is derived from the flow element container. This container consists of the elements `FlowElement`. A task in a process, in turn, is one of the possible activities that are nodes in the flow. This hierarchy is shown in Figure

2. The elements that allow to include information about the security policy are shown in Figure 2 in a given rectangle. The `SecuredTask` class has been introduced, which requires no additional attributes beyond the binding to the `SecurityLevel` class. Such a change in BPMN objects' structure allows for the inclusion of the tasks in a process that requires compliance with safety rules. The definition of `SecuredTask` class saved with XML Schema is shown below:

```
<xsd:schema>
…
<xsd:element name="securedtask"
  type="tSecuredTask"/>
    <xsd:complexType name="tSecuredTask">
    <xsd:complexContent>
        <xsd:extension base="tTask"/>
        <xsd:sequence>
           <xsd:element ref="securityLevel"
           minOccurs="1" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexContent>
    </xsd:complexType>
… </xsd:schema>
```

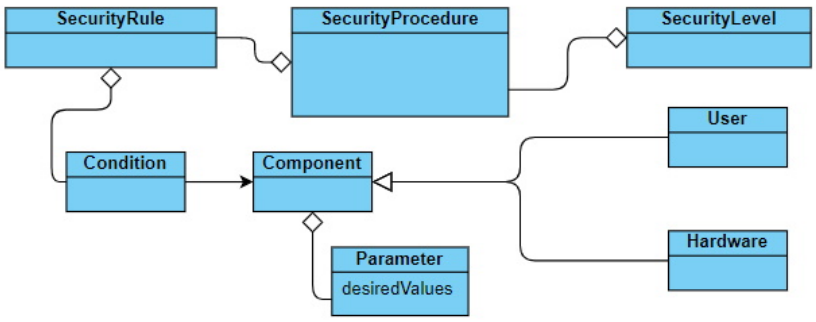

Figure 1. Class Structure for Defining the Security Policy

In the definition of `tSecuredTask` type the information about the `tTask` extended type is included together with the references to security policies. Precisely one level of security is involved with each `tSecuredTask` element. For the graphical representation of the security

level in the BMPN diagram, it was decided to use a text label in the upper right corner of the task symbol of security policy.

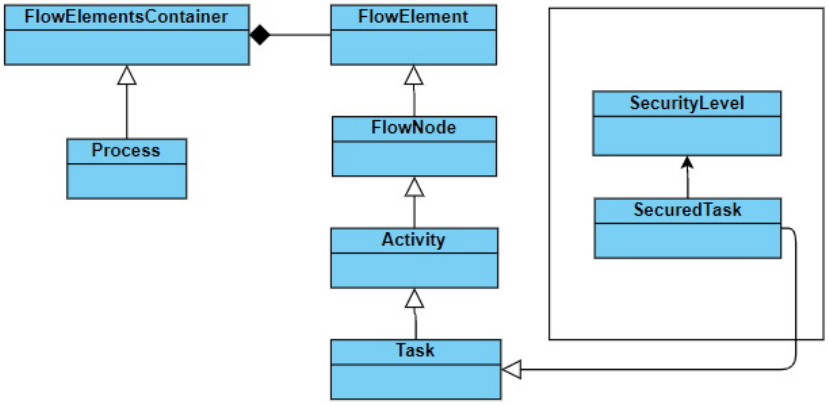

Figure 2. Extension of BPMN Class Structure

DISCUSSION AND CONCLUSIONS

The security policy described in section *Example of Security Policy* was presented using the notation proposed in (Salnitri et al. 2014). In the case of modelled process, each of the tasks has to be realized with confidentiality, secure account and privacy. The activities performed by the recruitment panel are additionally related to audibility. It makes it necessary to draw as many as forty connections on the BPMN diagram, which negatively affects its readability.

Apart from being less readable, using the symbols proposed in (Salnitri et al. 2014), it is not possible to define a security policy according to the model presented in the subsection *Definition of Information Security Policy*. It is not possible to indicate specific rules related to security procedures applied in the company. Some distinctions can be made with notes, but the number of notes would make the diagram even less legible (Figure).

This paper presented the security policy model that allows grouping into levels the security procedures used in a company. Each security procedure requires checking the specific conditions regarding the hardware or people involved in the business processes. Conditions refer

to having specific values by parameters that describe hardware or people. Due to the full freedom in determining the permissible values of these parameters and their number, it is possible to consider the complex security regulations and those that correspond to protection against emerging types of threats.

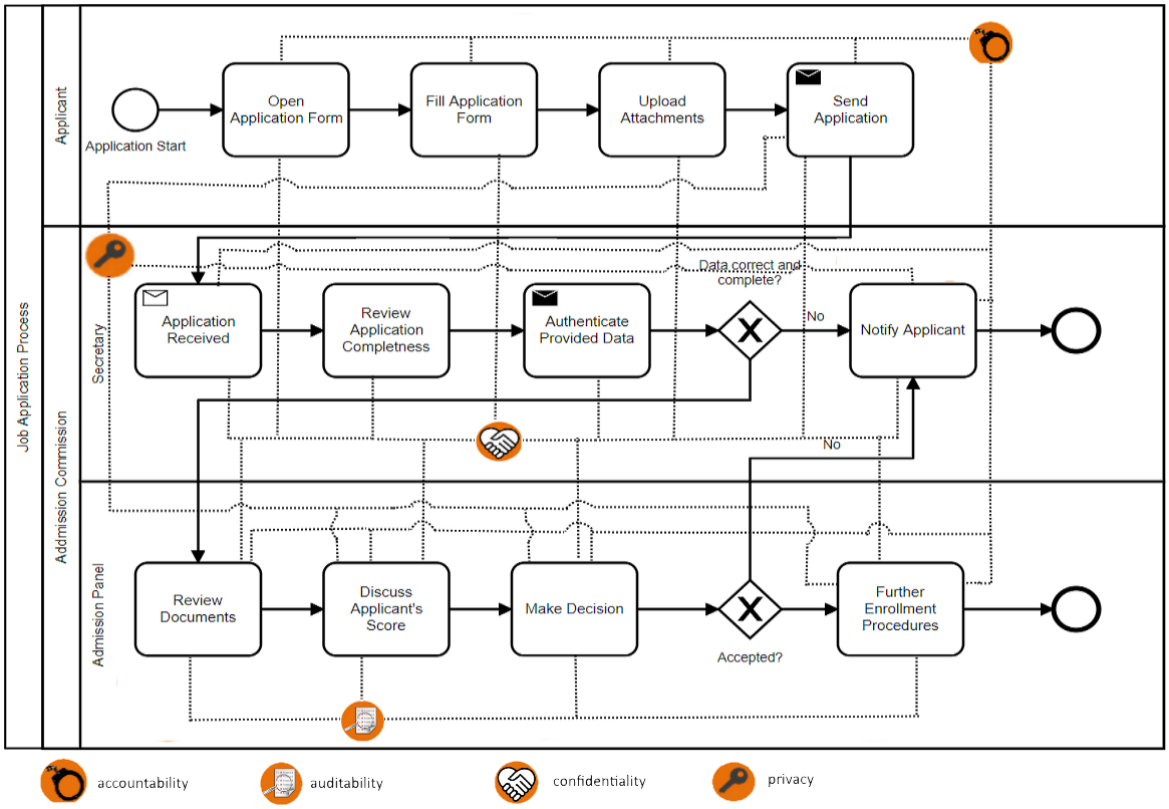

Figure 3. Presentation of Exemplary Recruitment Process with SecBPMN Notation

The proposed security policy model was transferred to the BPMN structure, which allowed its inclusion in diagrams created using this notation. Proposed improvement of BPMN is not complicated – it consists of including information at the security level in the tasks related to the implementation of security procedures. For this reason, the BPMN diagram remains legible.

The notations used so far allow only the inclusion of information on security-related activities in the BPMN diagram but do not bind them with specific security procedures. Although this allows the analysis of a diagram to notice that the need to verify security occurs

when performing certain tasks in the process, the SecBPMN notation does not allow for detailing this information in an understandable way. In further work, the authors will focus on the development of domain language that allows modelling the security policy, which can be presented using the BPMN syntax extension proposed in this paper.

REFERENCES

Acemyan, C. Z., Kortum, P., Xiong, J., and Wallach, D. S. 2018. "2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, SAGE Publications Sage CA, Los Angeles, USA, pp. 1141-1145.

Agostinelli, S., Maggi, F. M., Marrella, A., and Sapio, F. 2019. "Achieving GDPR compliance of BPMN process models," in *Proceedings of International Conference on Advanced Information Systems Engineering*, Springer, pp. 10-22.

Ahn, G. J., and Hu, H. 2007. "Towards realizing a formal RBAC model in real systems," in *Proceedings of the 12th ACM symposium on Access control models and technologies*, pp. 215-224.

Argyropoulos, N., Mouratidis, H., and Fish, A. 2019. "Enhancing secure business process design with security process patterns," *Software & Systems Modeling*, pp. 1-23.

Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., and Song, D. 2007. "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 598-609.

Barni, M., Droandi, G., Lazzeretti, R., and Pignata, T. 2019. "SEMBA: secure multi-biometric authentication," *IET Biometrics* (8:6), pp. 411-421.

Chang, J. F. 2016. *Business process management systems: strategy and implementation*, CRC Press.

Ding, S., Cao, J., Li, C., Fan, K. and Li,, H. 2019. "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access* (7), pp. 38431-38441.

Do, T.-X., and Kim, Y. 2019. "Topology-aware resource-efficient placement for high availability clusters over geo-distributed cloud infrastructure," *IEEE Access* (7), pp. 107234-107246.

Dumas, M., La Rosa, M., Mendling, J., and Reijers, H. A. 2013. *Business process management*, Springer.

Gaidels, E., Gaidukovs, A., and Matulevicius, R. 2018. "A Coarse-Grained Comparison of BPMN Extensions for Security Requirements Modelling," in *Proceedings of BIR Workshops*, pp. 170-181.

Hammi, M. T., Hammi, B., Bellot, P., and Serhrouchni, A. 2018. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security* (78), pp. 126-142.

Jeston, J., and Nelis, J. 2014. *Business process management*, Routledge.

Kumar, A. 2018. *Business Process Management*, Taylor & Francis.

Liang, Y., He, F., and Li, H. 2019. "An asymmetric and optimized encryption method to protect the confidentiality of 3D mesh model," *Advanced Engineering Informatics* (42), pp. 100963.

Lindsay, A., Downs, D., and Lunn, K. 2003. "Business processes – attempts to find a definition," *Information and software technology* (45:15), pp. 1015-1019.

Liu, B., Yu, X. L., Chen, S., Xu, X., and Zhu, L. 2017. "Blockchain based data integrity service framework for IoT data," in *Proceedings of 2017 IEEE International Conference on Web Services (ICWS)*, IEEE, pp. 468-475.

Ma, M., Shi, G., and Li, F. 2019. "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access* (7), pp. 34045-34059.

Maines, C. L., Llewellyn-Jones, D., Tang, S., and Zhou, B. 2015. "A cyber security ontology for BPMN-security extensions," in *Proceedings of 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, IEEE, pp. 1756-1763.

Maines, C. L., Zhou, B., Tang, S., and Shi, Q. 2016. "Adding a third dimension to BPMN as a means of representing cyber security requirements," in *Proceedings of 9th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, pp. 105-110.

OMG. 2013. "Business Process Model and Notation (BPMN), Version 2.0.2," Object Management Group, Technical report, Object Management Group.

Pitchai, R., Babu, S., Supraja, P., and Anjanayya, S. 2019. "Prediction of availability and integrity of cloud data using soft computing technique," *Soft Computing* (23:18), pp. 8555-8562.

Puthal, D., Wu, X., Nepal, S., Ranjan, R., and Chen, J. 2017. "SEEN: A selective encryption method to ensure confidentiality for big sensing data streams," *IEEE Transactions on Big Data*.

Rodriguez, A., Fernбndez-Medina, E., and Piattini, M. 2007. "A BPMN extension for the modeling of security requirements in business processes," *IEICE transactions on information and systems* (90:4), pp. 745-752.

Salnitri, M., Dalpiaz, F., and Giorgini, P. 2014. "Modeling and verifying security policies in business processes," *Enterprise, business-process and information systems modeling*, Springer, pp. 200-214.

Tchernykh, A., Schwiegelsohn, U., Talbi, E.G., and Babenko, M. 2019. "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *Journal of Computational Science* (36), pp. 100581.

Thillaiarasu, N., and ChenthurPandian, S. 2019. "A novel scheme for safeguarding confidentiality in public clouds for service users of cloud computing," *Cluster Computing* (22:1), pp. 1179-1188.

Thwin, T. T., and Vasupongayya, S. 2019. "Blockchain-based access control model to preserve privacy for personal health record systems," *Security and Communication Networks* (2019).

Tipton, H. 2019. *Information Security Management Handbook: Volume IV*, CRC Press.

Vayghan, L. A., Saied, M. A., Toeroe, M., and Khendek, F. 2019. "Microservice Based Architecture: Towards High-Availability for Stateful Applications with Kubernetes," in *Proceedings of IEEE 19th International Conference on Software Quality, Reliability and Security (QRS)*, IEEE, pp. 176-185.

Zareen, S., Akram, A., and Ahmad Khan, S. 2020. "Security Requirements Engineering Framework with BPMN 2.0. 2 Extension Model for Development of Information Systems," *Applied Sciences* (10:14), pp. 4981.

APPENDIX A – EXAMPLE OF A BUSINESS PROCESS IN EXTENDED BPMN NOTATION

The proposed extension of BPMN notation is illustrated in the example of the recruitment process for which the required diagrams were created using the proposed notation. The same process, taking into account the security-relevant requirements, is presented using selected BPMN extensions.

Business Process Description

For the practical purposes of this study, it was assumed that during the recruitment process an Applicant fills in the application form and attaches a certain number of attachments to it, e.g. in the form of necessary certificates confirming his/her professional qualifications or employment certificates from previous employers.

The submitted application form, along with the attachments, is carefully verified for completeness by the employer's secretariat. The secretary's employee is responsible for verifying the accuracy of data contained in the application form and in attachments. For this purpose, it contacts the previous employers and checks the authenticity of certificates confirming professional qualifications presented by the Applicant. If the application form is incomplete or any irregularities in the attachments are found, the secretary's employee informs the Applicant about it, and the process is interrupted.

If the application is complete and the data in attachments is correct, then the application is directed to the panel of recruiters who evaluate the Applicant's documents and then assess its usefulness in the company, granting the application a score. The application evaluation process ends with a decision. If it is refused, the Applicant is informed about it. Otherwise, further steps

related to the employment of the Applicant are carried out. The process described above is presented in figure 4.

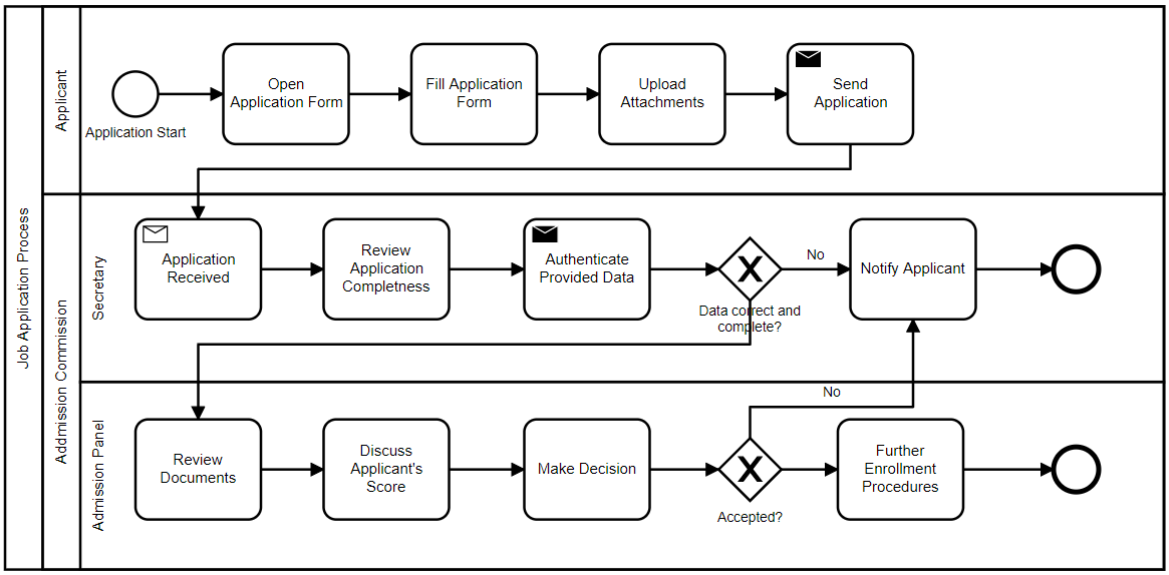

Figure 4. Example of BPMN Diagram Presenting the Recruitment Process

Example of Security Policy

Recruitment processes require the assurance of an appropriate level of security. In the presented example process, the main security assumption is the confidentiality of the Applicant's data and data protection during the recruitment process. The security policy elements in the presented example are as in Table 2.

For the purposes of the system, a set of security rules was created, as shown in Table 3. The rules R_1 and R_2 apply to servers operating in the company. Access to each of the servers is via an encrypted connection. Data stored on these servers is backed up each day. Access to the application software server is public, while the login and audit servers are accessible only from the internal office network. Rule R_3 applies to secretarial staff and members of the recruitment panel. They have to login into the system via LDAP, change their password at least once a

month, and have a password that is at least 10 characters long. The recruitment panel members must have encrypted data on local disks (rule R_4) and use an auditing system while making a decision (rule R_5). The rule R_6 applies to GDPR compliance, followed by company employees and job application software.

Table 2. Elements of Exemplary Information Security Policy

Element	Description
System	Recruitment system
Business Process	Job Application Process
Users	• Applicant (U_A) – responsible for preparing the job application. • Secretary Employee (U_S) – responsible for formal verification of received job application. • Admission Panel Member (U_{APM}) – responsible for score application, making employment decision and handling further steps in the enrolment process.
Hardware	• Applicant's computer (H_{AC}). • Secretary's computer (H_{SC}). • Admission Panel Members' computers (H_{APMC}). • Server with job application software (H_{JAS}). • Auditing Server (H_{AudS}) – responsible for recording the actions of specific Users. • Authentication Server (H_{AuthS}) – responsible for verification of employees' credentials.

Table 3. Rules for Business Process Elements in Exemplary Information Security Policy

Rule	Component	Parameter	Desired Values
R_1	H_{JAS}	Encryption	SSL, SHA-512
		Data Backup	Each day
		Access	Public
R_2	H_{AudS}, H_{AuthS}	Data Backup	Each day
		Access	Office network
R_3	H_{SC}, H_{APMC}	Authentication	LDAP
		Password Length	10
		Password Expiration	30 days
		Hard Disk Backup	Each 5 days

R_4	H_{APMC}	Hard Disk Encryption	Yes
R_5	H_{APMC}	Use of Auditing server	Yes
R_6	H_{JAS}, U_{APM}, U_S	GDPR Compliance	Yes

There are no specific rules for the Applicant' s computer, as it is not under the company's management. Based on the security rules given in Table 3, the security procedures were created. Four security procedures are distinguished in the presented example:

1. SP_1 – servers in the company are secured with an encrypted connection; only the server with the recruitment application is available to the public (rules R_1, R_2).
2. SP_2 – secretarial employees use secure passwords and make regular backups (rule R_3).
3. SP_3 – members of recruiting panel use secure passwords, regularly back up the data and use data encryption on the local disks (rules R_3, R_4, R_5).
4. SP_4 – company's employees comply with the principles of GDPR (rule R_6).

Three security levels were created: Basic, Normal and Increased: SL_{Base}, SL_{Normal}, and $SL_{Increased}$ with the following procedures: SL_{Base} – procedures SP_1 and SP_4, SL_{Normal} – procedures SP_1, SP_2 and SP_4, $SL_{Increased}$ – procedures SP_1, SP_3 and SP_4.

The BPMN diagram taking into account the described security policy is shown in Figure . For each of the tasks, a security level resulting from the assumed policy were assigned. The tasks performed by the Applicant received the *Basic* security level. The tasks performing by the Secretariat are assigned *a Normal* security level. An increased level of security is necessary for the completion of tasks by the recruitment panel. Sending the Applicant a notification about the decision made based on the decision of secretariat or recruitment panel requires only a basic level of security.

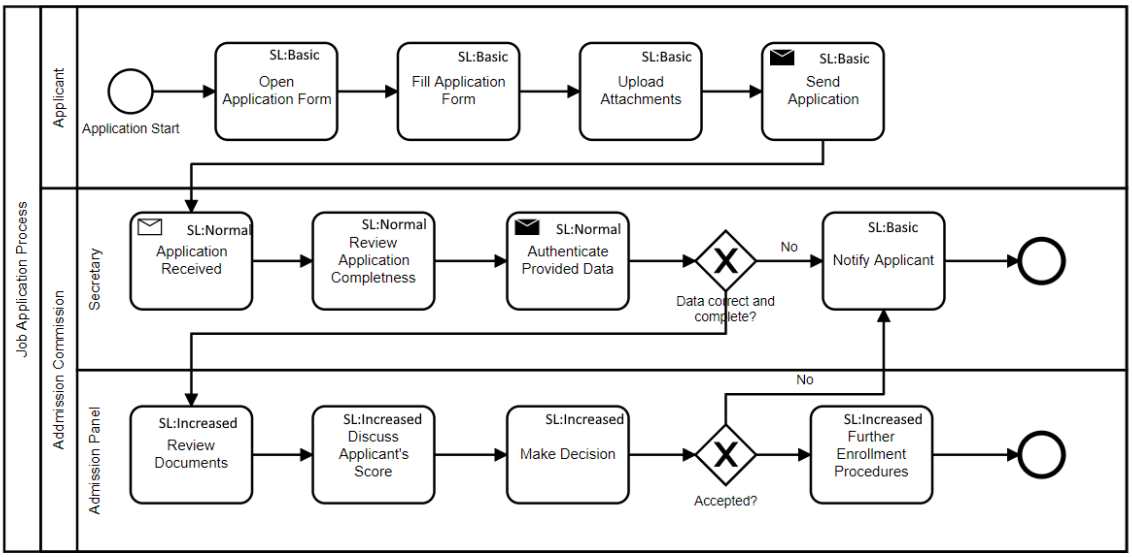

Figure 5. Presentation of Exemplary Recruitment Process with the Proposed BPMN Extension

The above example shows that the BPMN language extension proposed in subsection *Security Policy in BPMN Structure* in the field of modelling security procedures allows presenting the security policy defined in subsection *Definition of Information Security Policy*.