International Journal of Scholarly Papers for Media and Communication

ISSN 1800-7074 (print)
ISSN 2536-5622 (online)

Varga, M., Kujundzic, M. (2022), „Innovative Technologies of Web Services and Security Protocols", *Media Dialogues / Medijski dijalozi*, Vol. 15, No. 4, pp. 35-49.

Innovative Technologies of Web Services and Security Protocols

Assistant professor, MATIJA VARGA

North University, University of Applied Sciences Baltazar Zapresic

e-mail: mvarga@unin.hr

MARIO KUJUNDZIC, bacc. inf. tech.

University of Applied Sciences Baltazar Zapresic

e-mail: mariokujundzic993@gmail.com

ARTICLE INFO	Received: May 10, 2022 / Revised from: April 10, 2022 Accepted: June 10, 2022 / Available online: October 15, 2022
DOI	10.14254/1800-7074/2022.15-4.3

ABSTRACT

The research paper on "Innovative Web Services Technologies and Security Protocols" will explore: (a) the purpose of the SOAP protocol, (b) the shortcomings of the SOAP protocol, (c) the existence of possible security vulnerabilities within the SOAP protocol and (d) protection options. In addition to the research part, the paper will also apply the scientific method of content analysis based on which certain definitions of WEB services will be given, such as: XML, XACML, JSON, AJAX and REST. Also, theoretically will be explained in detail: web services, web services model with security standards and protocols such as: AJAX protocol, SOAP protocol, IPSec protocol and REST state transfer. In addition to these protocols and XML as an extensible language for tagging data and documents, an indispensable part of web services are formats such as: HTML 5.3 and JSON open standard for formatting data when transferring between applications that will also be covered by research. In addition to the above, various protocols used by IPSec will be presented in the paper, such as: AH protocol, ESP protocol and IKEv2 protocol. The paper will also present the results of a survey on the topic: "Web application programming".

KEY WORDS: *Web services, Models, XACML, JSON, IPSec, REST.*

INTRODUCTION

This research paper on "Web services technologies and security protocols" explored: what is the purpose of SOAP protocols, shortcomings of SOAP protocols, the existence of security vulnerabilities with in SOAP protocols, security capabilities, the model of SOAP protocols and security protocols. Innovative technologies that create web-based applications that enable numerous web services are useful for every end user because in most cases a study was made on the purpose and objectives of implementing innovative web applications that provide many benefits for users. A protocol is a pre-arranged procedure (given the time and place) that needs to be followed in a particular situation.

There are generally different types of protocols. Internet protocols are protocols that are used exclusively for the transmission of data within a computer network and use source and destination nodes to ensure communication with data over a computer network. It is common knowledge that data within a computer network is sent in datagrams. In addition to the research part, the paper also uses the scientific method of content analysis based on which certain definitions of WEB services are defined, such as: (1) XML, (2) AJAX, (3) SOAP and (4) REST and the scientific modelling method used to model the principles of operation. SOAP protocol and SOAP message structure and RESTful Web Service.

Also, theoretically explained in detail: (a) web services and (b) protocols such as: (a) AJAX protocols, (b) SOAP protocols and (c) REST state transfers. In addition to the mentioned protocols and XML as an extensible language for marking data and documents, an indispensable part of web services are formats such as: (a) HTML 5.3 and (b) JSON open standard for formatting data for transfer between applications that are also included in the research. JSON is a JavaScript Object Notation, i.e. JSON is an open standard for formatting data when transferring between applications and has human-readable syntax. JSON stores data in the form of attributes and values, and can also have a field as a data type. JSON is out of JavaScript and is supported by many programming languages. In web services, the protocols used are of great importance because they tell how the data is transmitted and how the application communicates over the Internet. Some of the more important and popular protocols are: (a) AJAX, (b) SOAP and (c) REST (representative state transfer). In addition to the presented innovative web technologies, this research presents the results of an online survey on the topic: "Web application programming" obtained by applying the scientific survey method.

1. SOAP PROTOCOL AND SECURITY PROTOCOLS

SOAP (Simple Object Access Protocol) protocol is a basic communication protocol intended for the exchange of text messages in web services. It describes the way in which the message will be formed during transmission by some of the transport protocols and the way in which the same message will be exchanged and processed between applications (www.w3.org, 2021). One of the most important protocols is IPSec, i.e. the Internet security protocol. For the purpose of data protection on the network layer of the reference OSI model, the IPSec protocol is used. The IPSec protocol provides basic security requirements such as: (a) authenticity, (b) confidentiality, and (c) integrity. The IPSec protocol can be configured in tunnel or transport mode. The transport mode only protects the data field of the IP datagram, while the tunnel mode protects the entire IP datagram. In addition, it ensures integrity and undeniability. Because the IP protocol provides end-to-end communication channel service, protecting the channel at the same level using IPSec allows it to be independent of the lower layers. This means that communication devices on the path between the two entities do not have to support IPSec, which allows the use of IPSec regardless of the way the physical layer and the data layer are implemented (www.cis.hr, 2022). IPSec (Internet Protocol Security) is a standard and set of protocols (optional for IPv4 and mandatory for IPv6) that include traffic protection mechanisms at the third layer level of the OSI network model.

IPv4 is the Internet Protocol version 4, while IPv6 is the Internet Protocol version 6. The main driver for the adoption of IPv6 has been the depletion of IPv4 addresses in certain parts of the world (Hovav et al., 2011). IPv4 is the earlier version of IPv6. IPv4 consists of 32 bits long addresses and each unique address is assigned

to each device so data can be transmitted to that specific address. Due to large number of growths in electronic devices, IPv4 addresses was not enough to cover all the devices. To resolve the issue IPv6 introduced which consists of 128 bits long address which can handled billions of devices and more than that and assign each device different unique address. IPv6 can handle more devices than the IPv4 and it's also easy to connect devices and transmit information from one device to another. Apart from connection of more devices IPv6 is also provide more efficient routing as compared to IPv4 (Anwar and Ghumman, 2019). IPv6 is the solution which is a new IP address format. IPv6 finds out more reliable and useful as compared to IPv4 in assigning addresses of devices routing of networks, security of information and data, translation of network address and also in support of configuration of protocol (Anwar and Ghumman, Ibid.).

In IPv4 fragments are handled by the router where as in IPv6 fragmentation is handled by the source device. IP version 4 supports broadcast rather than multicast whereas IPv6 supports multicast which means IPv6 can sent different packets in different directions simultaneously at a same time which saves network bandwidth. In IPv6 address of devices auto configure and assigned automatically to devices which are available where as in IPv4 you need to configure addresses of each device which is difficult to assign and also time consuming task. Dual Stack can process both IPv4 and IPv6 traffic simultaneously. Dual Stack devices like PC, a router or a server and other IoT (internet of things) can support both IPv4 and IPv6 (Anwar and Ghumman, Ibid.). IPSec stands for Internet Protocol Security. IPSec is an extension to the IP which provides security to the IP and the upper-layer protocols. IPSec is a collection of protocols designed by (IETF) to provide security at the network level. IPSec helps to create authenticated and confidential packets for the IP layers. IPSec Security controls exist for network communications at each layer of the TCP/IP model. Data is passed from the highest to the lowest layer, with each layer adding more information. IPSec Controls at this layer apply to all applications and are not application-specific. Network layer controls such as IPSec provide a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications (Kadhum M. Al-Qurabat, A., 2022). IPSec operates in one of two different modes (Figure 1).

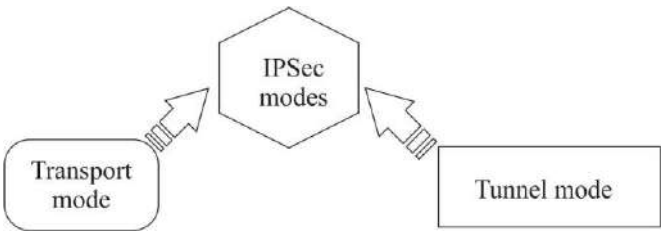

Figure 1. IPSec Modes
Source: Adapted to Kadhum & Al-Qurabat, 2022.

Figure 1 shows that IPSec in the transport mode does not protect the IP header, does not protect the whole IP packet, it only protects the information coming from the transport layer. In this mode, the IPSec header and trailer are added to the information coming from the transport layer. The IP header is added later. IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header. The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host. Benefits of IPSec are (Kadhum M. Al-Qurabat, A., 2022):

- strong security that can be applied to all traffic crossing,
- the perimeter,
- traffic within a company or workgroup does not incur,
- the overhead of security-related processing,
- IPSec can be transparent to end users,
- IPSec is transparent to applications, no need to change software on a user or server system when implementing it in the firewall or router,
- IPSec can provide security for individual users if needed.

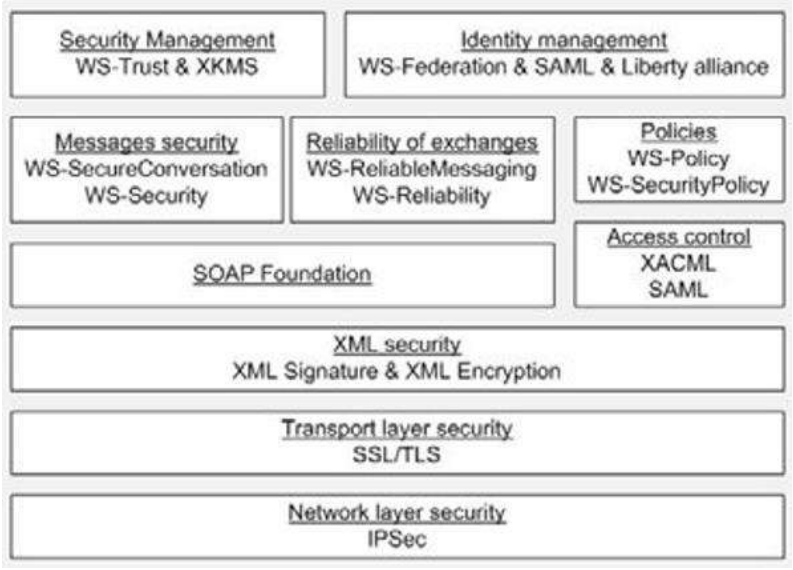

Figure 2. Web Services Security standards

Source: Mohamed et al., 2009.

Securing Web Services consists in providing security services (authentication, confidentiality, integrity, etc.) to the exchanged messages. This security could be introduced between two endpoints at the transport layer (SSL/TLS) or at the network

level (IPSec). However, these two protocols become inappropriate to secure WS based exchanges; because these last could involve many entities where each of them may need to access some parts of the exchanged messages while access to other parts may be prohibited. Hence, security standards for WS were specified (Figure 2) (Mohamed and Francine, 2009).

Based on Figure 2, Web Services Security standards include: (1) security management, (2) identity management, (3) message security, (4) reliability, (5) security policies, (6) SOAP foundations, (7) access control, (8) XML security (XML signature and encryption), (9) transport layer security (SSL and TLS), and (10) network layer security (IPSec).

The eXtensible Access Control Markup Language (XACML) (Figure 2) is the original standard for expressing access control policies and permits to express access control rules on the basis of a requester's properties. Although XACML enjoys large adoption in industry due to its simplicity and its powerful extension mechanism, it has several limitations. In particular, there is no support for certified credentials nor does it allow for dealing with unknown requesters. Rather, it is assumed that requesters provide all their properties together with the access request. However, this poses significant privacy risks for the requesters (Ardagna, et al., 2010). Servers host resources and protect them with policies expressed in an extended version of XACML. A server host is an IT service while a server is a server computer that provides clients with all the necessary information that most clients (client computers) naturally need. Hosting as a term means hosting web pages, i.e. the entire contents of web pages on web servers in order to be available to as many users of information as possible. If there are more users for certain information, the information is more valuable, i.e. it has more value. Access to different servers is determined by ports. Users requesting access to a resource receive the relevant policy, which describes the requirements on the requester's credentials in order to be granted access. The policy may include requirements on multiple credentials at the same time, meaning that multiple credentials have to be presented in order to obtain access, and may include provisional actions, i.e., actions that the requester needs to full fill prior to being granted access (Ardagna, et al., 2010).

SAML bindings map the SAML protocols onto standard lower level network communication protocols used to transport the SAML assertions between the identity provider and service provider. Some example bindings used are: (1) HTTP Redirect Binding – uses HTTP redirect messages, (2) HTTP POST Binding – defines how assertion scan be transported using base 64-encoded content, (3) HTTP Artefact Binding – defines how an artefact is transported to the receiver using HTTP, (4) SOAP HTTP Binding – uses SOAP 1.1 messages and SOAP over HTTP (Lewis, 2009). It is common knowledge that HTTP hypertext transfer protocol is a protocol used to exchange data packets between clients (personal computers) and www servers and allows the content of web pages to be sent to recipients (clients).

To ensure the authentication, integrity and reliability of communication, IPSec uses three different protocols: (1) AH, (2) ESP and (3) IKEv2:

- AH (Authentication Header) protocol for ensuring the inviolability of data and their authorization,
- ESP (Encapsulated Security Payload) protocol enables encryption and inviolability of data,
- The IKEv2 protocol is used to create and distribute cryptographic keys.

IKEv2 is an improved version of the IKEv1 protocol in terms of security (lower risk of DoS attacks) and simplicity (refers to the simplification of the protocol which facilitates its application) (www.cis.hr, 2022). The IKEv2 protocol is a request/ response protocol working on top of the UDP protocol. Each IKEv2 protocol entity sends and receives request and response messages, which are composed of a header and one or more payloads, depending on the particular message in question (Gros and Glavinic, 2022). The request message and its response are marked as information exchange. When the SA needs to be established, an IKEv2 daemon (called an initiator because it initiates communication) sends a request to another IKEv2 daemon (called Responder is responding). The first exchange aims to establish IKE SA which protects all further communication between these two implementations of the IKEv2 protocol. This first exchange is the only open text, while all remaining messages, except the header, are encrypted, i.e. encrypted by a certain algorithm. In another exchange, two IKEv2 demons authenticate each other and establish two SAs. From that point on, these two IKEv2 daemons can establish additional Child SAs, rekey and delete old ones, etc. To finish any further communication IKEv2 daemons delete the IKE SA, which also deletes any associated Child SAs (Gros and Glavinis, 2022).

The most well-known protocols that are in the transport layer of the ISO OSI reference model and are very important for sending and receiving data are: TCP and UDP protocols. Both of these protocols are used to send bits over the network, but each has one important difference. The TCP protocol is the most commonly used protocol and is specific in that it relies on reliability, i.e. checks and waits for a response on the other hand whether the packet arrived with some bit loss or was fully received as it was sent.

It is used for processes that require reliability and some kind of security, such as e-mail, connecting to some other networks. The UDP protocol is the opposite of the TCP protocol, i.e. it binds to speed and when data is sent, it does not wait for feedback on whether the bit or packet arrived in full or latency occurred, i.e. the loss of part of the packet. It is most often used for streaming or playing video or audio, where if a piece of data is lost, it continues to take further steps or reduces the quality of the recording. It is also often used with DNS servers, where the speed of synchronizing the server with computers (Clusters) is important. These two protocols are located in the transport OSI layer and are very important for sending and receiving

data. The language in which SOAP messages are written is called Extensible Markup Language (XML). There are different types of messages in SOAP, the most famous being the Remote Procedure Call (RPC). The protocol is best managed in an environment where there is a formal agreement of communication between the application and services, and thus in operations where the state of services or applications is monitored (Rouse, 2022).

The standard HTTP protocol makes it easier for the SOAP model to go through firewalls and proxy servers without additional modifications. In order for the connection to SOAP web services to be secure, it is necessary to set the service URL to HTTPS so that all data is transmitted over a secure layer, i.e. SSL (Secure Socket Layer). SSL is a protocol that enables HTTPS and relies on asymmetric encryption. In asymmetric cryptographic systems, there are two types of cryptographic keys - public and secret cryptographic key. The public cryptographic key is used exclusively for encryption, and the secret for decryption. The public and secret cryptographic keys form a unique pair. A unique secret key is added to each public key. In practice, it is very difficult, almost impossible, to calculate the other by knowing one of them. It works in such a way that the client, in this case the application that sends the requests, gets the public key via an SSL certificate and uses it to initiate secure communication with the web service. While, on the other hand, the web service keeps its private key secret and decrypts the received requests with it.

2. THE ROLE OF AJAX TECHNOLOGY AND REST SERVICES

The role of REST (Representative state transfer) and the advantages over the SOAP protocol are: (1) faster response to demand, (2) lower implementation cost and (3) easier maintenance of server side communication and (4) less memory usage (Šimec and Lozić, 2014). The REST protocol can use several different responses (XML, JSON, etc.), it uses data. Display code comparison, i.e. examples of data in JSON and XML:

Example 1:

```
{
"firstName" : "Matija",
"lastName" : "Varga",
"room" : "4021",
"phone" : "098303421",
"_links" : {
"self" : { "href" : "http://localhost:8080/persons/2" }
}
}
```

Example 2:

```
<person>
        <firstName>Matija</firstName>
        <lastName>Varga</lastName>
        <room>4021</room>
        <phone>2098303421</phone>
        <links>
                <link>
                        <rel>self</rel>
                        <href>http://localhost:8080/person/3</href>
                </link>
        </links>
</person>
```

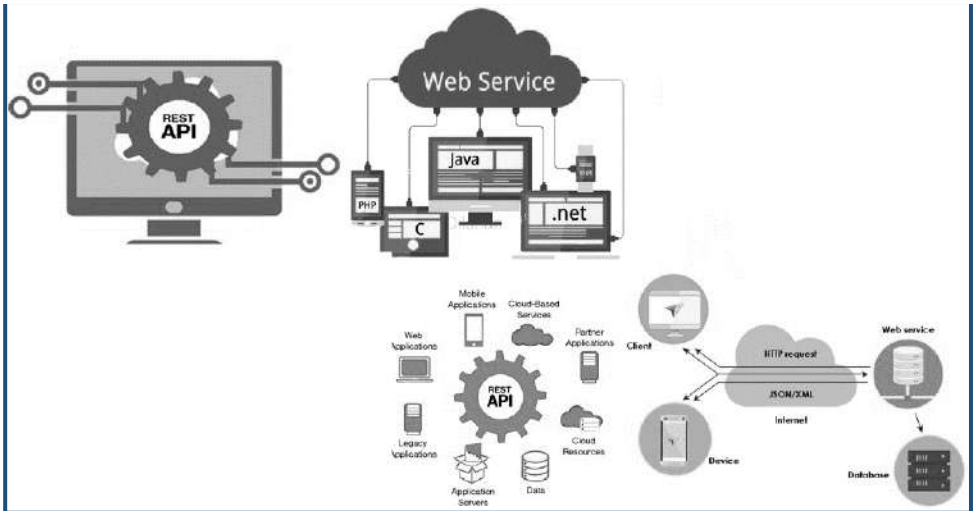

Figure 3. RESTful Web Service

Source: Ramesh, 2021.

REST (Representative state transfer) or "Representative state transfer" is a software architecture that defines predefined rules and restrictions that must be met when creating Web services (Intriago, 2022). REST services provide good temporary caches when using GET calls (Simec and Lozic, 2014). Currently, the best solution for communication between technologies is the REST (Representational state transfer) protocol. REST has taken excellent capabilities from SOAP protocols such as neutrality, i.e. the ability of programming languages such as: C / C ++, C #,

Java and similar programming languages, to communicate independently of the operating system (MS Windows family, Linux, etc.) (Šimec and Lozić, 2014). REST arose from the WWW (World Wide Web) technology, i.e. services, by introducing certain restrictions. These constraints form the basic principles of the REST model (Figure 3) that determine how resources on the global Internet can be used. The motivation for introducing these constraints is to create a finite system that takes full advantage of the web architecture to make the system work better. Since the mentioned non-standard web services often implement part of the theoretical principles of the REST model, they are called RESTful web services. This emphasizes that some REST principles are used but not all REST principles again.

Figure 3 shows RESTful Web services that include applications created in programming languages such as: (1) Java, (2) pHp, (3) C programming language, and * .net. Java is a popular programming language (www.w3.org, 2021). Java is used to develop mobile apps, web apps, desktop apps, games and much more (www.w3.org, 2021). PHP is currently one of the most popular programming languages, widely used in both the open source community and in industry to build large web-focused applications and application frameworks (Siame and Kunda, 2017). C is a general-purpose programming language, developed in 1972, and still quite popular (www.w3.org, 2021). Also, communication between client and device, web services and client, devices and web services, and web utilities and the database they use is shown. The model displays an HTTP request. The XMLHttpRequest object is part of the API that can be used through JavaScript, but also other scripting languages in Web browsers. The XMLHttpRequest object is used to transfer XML or other textual data to and from the server using the HTTP protocol, i.e. establishing an independent communication channel between the Web site on the client and server side. The data returned by the XMLHttpRequest object call can usually be: XML, HTML or JSON.

This object is an important part of AJAX applications, i.e. their ability to implement a dynamic interface. In addition to the principle of REST, as each resource has a unique identifier, there are the following principles such as: (1) interconnection of resources, (2) use of standard methods, (3) resources with multiple representations and (4) communication without maintenance. Asynchronous JavaScript and XML or AJAX is a set of related technologies for web application development. The use of these development techniques increases the interactivity on the website, and CSS is most often used for the presentation. It is possible to use them with server technologies, but most often everything is done on a client basis, without the need to reload data and additional transfer from the server. JavaScript is a simple, interpreted scripting language designed primarily for the development of interactive HTML pages. The core of JavaScript is included in most of today's browsers such as Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari and others). JavaScript allows you to perform certain actions in otherwise static HTML documents, such as interacting with a user, changing browser window properties, or dynamically crea-

ting HTML content. JavaScript is not a simplified version of the Java programming language.

3. VIEW SURVEY RESULTS ON THE TOPIC: "WEB APPLICATION PROGRAMMING"

The aim of the survey was to determine: (a) which of the listed programming languages dedicated to creating applications for smartphones and tablets were used by respondents, (b) which of the listed programming languages dedicated to creating applications for smartphones and tablets are most commonly used, (c) which of the listed descriptive languages and / or scripting languages dedicated to the creation of responsive web pages were used by the respondents, (d) which of the listed descriptive languages and / or scripting languages dedicated to creating responsive web pages are most often used according to respondents and (e) whether respondents have so far used languages like ASP.net or Ruby to create websites. The sample consists of respondents who deal with the design and development of websites and applications.

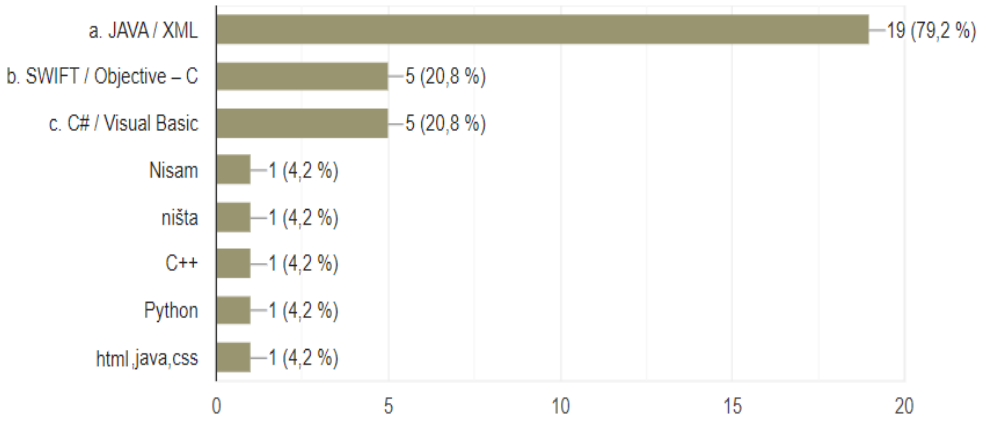

Figure 4. A review of the listed programming languages dedicated to the creation of applications for smartphones and tablets that the respondents used

Figure 4 shows which of the listed programming languages dedicated to creating applications for smartphones and tablets were used by the respondents. 79.2% of respondents used Java and XML the most, while SWIFT and objective C language were in second place.

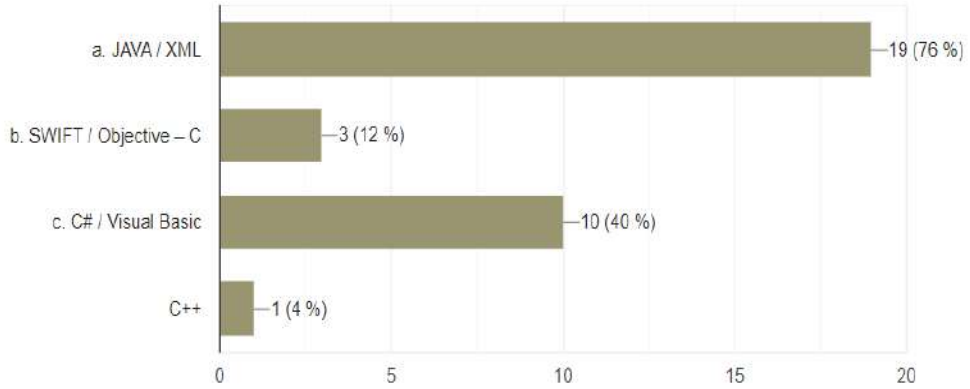

Figure 5. A review of the listed programming languages dedicated to the creation of applications for smartphones and tablets that are most often used according to the respondents

Figure 5 shows which of the listed programming languages dedicated to creating applications for smartphones and tablets are most often used according to the respondents. The majority of respondents (76%) think that they are most often used to create applications for smartphones and tablets JAVA and XML, while they also think the least respondents (12%) think that they use SWIFT and Objective C.

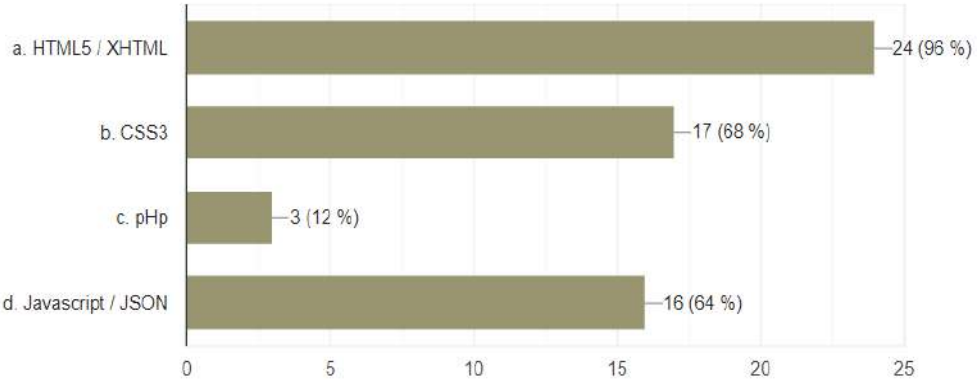

Figure 6. Display of the listed descriptive languages and / or scripting languages dedicated to the creation of responsive web pages that the respondents used most often

Figure 6 shows which of the listed descriptive languages and / or scripting languages dedicated to creating responsive websites were used by the respondents. Most respondents (96%) used HTML5 and XHTML.

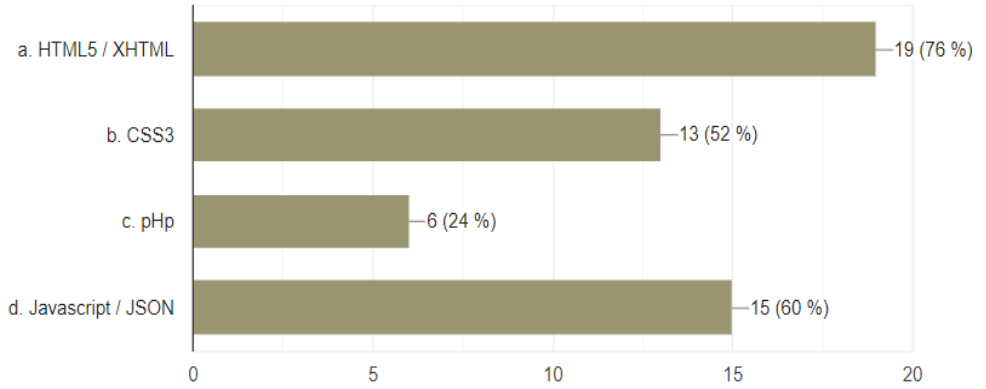

Figure 7. Presentation of the listed descriptive languages and / or scripting languages dedicated to the creation of responsive web pages that are most often used according to the respondents

Figure 7 shows which of the listed descriptive languages and / or scripting languages dedicated to creating responsive websites are most often used according to the respondents. According to the opinion (76%) of respondents, HTML5 and XHTML are most often used, while 52% of respondents believe that CSS3 is most often used when creating responsive web pages.

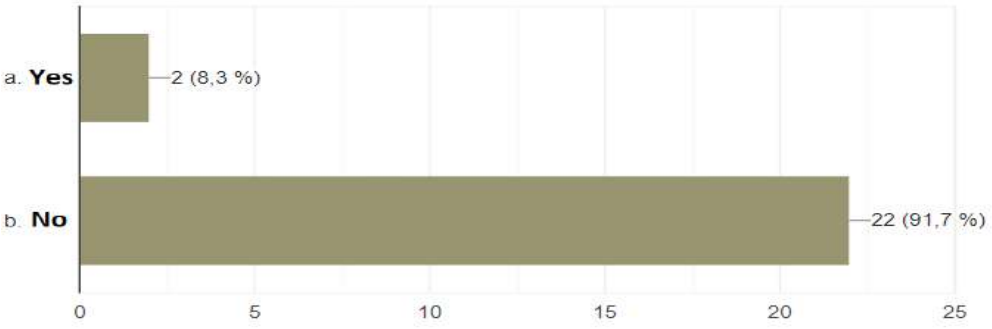

Figure 8. View the results of whether respondents have so far used languages such as ASP.net or Ruby to create websites

Figure 8 shows whether respondents have so far used languages such as ASP.net or Ruby to create websites. The majority of respondents (91.7%) chose the no option, while 8.3% of respondents chose the yes option.

CONCLUSION

Research work has investigated: (a) the purpose of the SOAP protocol, (b) the shortcomings of the SOAP protocol, (c) the existence of security vulnerabilities within the SOAP protocol, and (d) the possibility of protection. Also, the model of SOAP operation and security network protocols with emphasis on the IPSec protocol was investigated. The model name: "RESTful Web Service" is modelled by the scientific method of modelling and shows RESTful Web services that include applications created in programming languages such as: Java, pHp, C programming language and * .net- and etc. . Research based on the presented models proves that Internet and web technologies are closely related to the provision of web services and are of great importance network security protocols that enable data protection at the network layer (reference OSI model) and provide basic security requirements such as:) authenticity, (2) confidentiality and (3) data integrity.

These security requirements are ensured by the IPSec protocol using:

- AH (Authentication Header) protocol for ensuring the inviolability of data and their authorization,
- ESP (Encapsulated Security Payload) protocol that enables encryption and inviolability of data, and
- IKEv2 protocol used to create and distribute cryptographic keys.

It is also worth mentioning that the SSL protocol also enables HTTPS and relies on asymmetric encryption, which can also use public and secret cryptographic keys. Most respondents (79.2%) use JAVU and XML to create applications for smartphones and tablets, while respondents also chose the most commonly used programming languages dedicated to creating applications for smartphones and tablets JAVU and XML (76%). Most respondents (96%) of descriptive languages and / or scripting languages dedicated to creating responsive websites used HTML5 and XHTML, while the most commonly used (76%) also HTML5 and XHTML (according to respondents). Also, it should be noted that the majority of respondents (91.7%) have not used languages such as ASP.net or Ruby to create websites.

REFERENCES

Anwar, F., Ghumman, F. (2019). “Effects of IPV4/IPv6 Transition Methods in IoT (Internet of Things): A survey”, *Rochester, SSRN Conference* (May 17, 2019). https://ssrn.com/abstract=3402664 or http://dx.doi.org/10.2139/ssrn.3402664.

Ardagna, C.A. et al. (2010), “Enabling Privacy-preserving Credential-based Access Control with XACML and SAML”, *10th IEEE International Conference on Computer and Information Technology*, pp. 1090-1095, doi: 10.1109/CIT.2010.199. (3.4.2022.).

Gros, S., Glavinic, V. (2022), "Architecture of An Ikev2 Protocol Implementation", http://www.zemris.fer.hr/~sgros/publications/conferences/cnis2007.pdf. (21.3.2022.).

Hovav, A., Hemmert, M., Kim, Y. (2011), "Determinants of Internet standards adoption: The case of South Korea", *Research Policy,* Vol. 40. pp. 253-262.

Intriago, F. (2022). „JSON Tutorial", https://www.academia.edu/19435559/JSON_ Tutorial (28.1.2022.).

Kadhum M. Al-Qurabat, A. (2022), "IP Secury (IPSec)", https://www.researchgate. net/publication/320357573_What_is_ IPsec. (15.3.2022.).

Lewis, J. E., Lewis, K. D. (2009). "Web single sign-on authentication using SAML", *International Journal of Computer Science Issues,* Vol. 1, pp. 41-48. doi.org/10.48550/arXiv.0909.2368.

Mohamed, A.C., Francine, K. (2009), "A Secured Service Level Negotiation in Ubiquitous Environments", *International Journal of Communication Networks and Information Security,* https://www.researchgate.net/profile/FrancineKrief/ publication/220178854_A_Secured_Service_Level_Negotiation_In_Ubi quitous_Environments/links/5522b7c80cf29dcabb0ed9bd/A-Secured-ServiceLevel-Negotiation-In-Ubiquitous-Environments.pdf? origin=figuresDialog_download. (22.3.2022.).

Ramesh, D. (2021), "RESTful Web services", https://medium.com/@ dilshanramesh 81/restful-web-services-35a96401b42b (16.11.2021).

Rouse, M. (2022), "SOAP (Simple Object Access Protocol)", https:// searchapparc hitecture.techtarget.com/definition/SOAP-Simple-ObjectAccessProtocol (28.1.2022).

Siame, A. Kunda, D. (2017), "Evolution of PHP Applications: A Systematic Literature Review", *International Journal of Recent Contributions from Engineering, Science & IT,* Vol. 5. No. 28. 10.3991/ijes.v5i1.6437. (3.4.2022).

Simec, A., Lozic, D. (2014), "Smart communication on the Internet via the REST protocol", *Mipro 2014*, Opatija, pp. 1498-1505. VPN server comparison. CCERT-PUBDOC-2008-11-246. Croatian Academic and Research Network. https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-11-246.pdf (17.3.2022).