XXI INTERNATIONAL SCIENTIFIC-EXPERT CONFERENCE ON RAILWAYS
RAILCON '24
October 10-11, 2024; Niš, Serbia

Original scientific paper DOI: 10.5937/Railcon24059P

# ANALYSIS OF CYBER SECURITY MECHANISM IN RAILWAY COMPANIES IN ELECTRONIC BUSINESS PROCESSES

Zoran G. PAVLOVIĆ [1] [0000-0001-6076-1811]
Veljko RADIČEVIĆ [2]
Miloš MILANOVIĆ [3]
Adela SULEJMANI [4]
Marko BURSAĆ [5]

***Abstract –*** *Railway companies, in accordance with their vision and mission, have the basic task of traffic management as well as the transportation of users and goods. In order to regularly carry out business tasks, railway companies increasingly apply the available systems and technologies of electronic business. Basically, electronic business enables the modern implementation of business activities through digital channels. Today, traditional business models are being completely replaced by innovative digital models based on a large percentage of the use of computer systems in both companies and individuals in their homes. This innovative electronic business system requires the protection and security of all participants in digital communication processes. This paper presents cyber security mechanisms that can be applied by railway companies in business. The main goal is a comparative analysis of the protection mechanism, which includes the components of traditional protection systems that are already in place, up to modern ones that include the application of blockchain technology.*

***Keywords - protection mechanisms, cyber security, cryptography, innovative methods of railway e-business.***

## 1. INTRODUCTION

The development of the Internet leads to the application of new technologies in the business of transport companies as well as railways. Railway companies already use the Internet as a network of all networks for the realization of daily business tasks, communication with partners and interested users. The provision of services and the realization of business tasks in e-business enables a large number of operations to be performed faster, more accurately, and more reliably, which involve sending instructions or orders in the form of digital messages. In order for this trend to be on the rise, great attention must be paid to cyber security. Users of the service have the greatest apprehension and aversion to electronic business because they do not have enough information about how secure digital transactions are via the Internet. Employees of the railway company have to learn through various trainings how and in what way to safely participate in the interaction that involves electronic business processes.

At the beginning, the paper includes an analysis of cyber attacks that may occur in the railway company. Redirecting, modifying or fabricating messages in electronic business processes can cause large-scale damage where, in addition to the alienation of financial resources when paying for a certain service, there can also be human casualties. However, this paper will present algorithms and standards that will be replaced by blockchain technology in the near future to increase security in the event of cyber attacks.

[1] Academy of Technical and Art Applied Studies, Departments School of Railroad Transport, Starine Novaka 24, 11000 Belgrade, Republic of Serbia zoran.pavlovic@vzs.edu.rs
[2] Academy of Technical and Art Applied Studies, Departments School of Railroad Transport, Starine Novaka 24, 11000 Belgrade, Republic of Serbia veljko.radicevic@vzs.edu.rs
[3] Academy of Technical and Art Applied Studies, Departments School of Railroad Transport, Starine Novaka 24, 11000 Belgrade, Republic of Serbia milos.milanovic@vzs.edu.rs
[4] Academy of Technical and Art Applied Studies, Departments School of Railroad Transport, Starine Novaka 24, 11000 Belgrade, Republic of Serbia adela.sulejmani@vzs.edu.rs
[5] Academy of Technical and Art Applied Studies, Departments School of Railroad Transport, Starine Novaka 24, 11000 Belgrade, Republic of Serbia marko.bursac@vzs.edu.rs

## 2. THE NEED FOR CYBER SECURITY AND ATTACK MODALITIES

The application of innovative electronic business technologies ensures new ways of exchanging information between interested parties in daily activities [1][2], as well as the application of protection mechanisms. It is basically the application of computers (hardware and software) and the Internet to exchange information in the form of messages. The basic purpose of computer systems is the collection, processing and storage of data, as well as the application of available security mechanisms of all processes in electronic business. In the past, the development of computer systems led to the need for mutual data sharing, which was achieved through networking where there was a possibility of attack. In the world of science, new technical-technological improvements in computer systems are developed every day (e.g. electronic business, 5G and the announcement of 6G networks, artificial intelligence, the Internet of intelligent devices, expert systems, machine learning, etc.). The interested state and private sector, in order to improve daily activities, sees a chance to improve the current operational work through the application of existing and innovative solutions. In essence, the basis is mutual connection and exchange of data and information between interested parties in a protected and safe way [3-6].

In addition to the mentioned usual flow of information, there may be an attack on the availability of the system where there is an interruption in communication (figure 1) [7]. The easiest form of attack can be the interruption of a communication line, damage to a hardware component, obsolescence of a software program, etc.

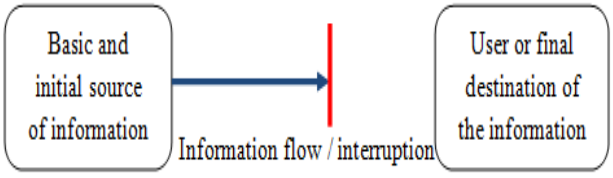


*Fig.1. Interruption of the flow of information*

Attacks related to integrity (content) involve modifying the message. Then there is a change in the content of the message, which can be a notification, information or even an order. In any case, the recipient of the message does not receive the original message, but a modified one, where the essence of the message and its meaning are changed. The modification of information in the form of a message (e-mail, electronic invoice, electronic bill of lading in traffic, electronic purchase order, etc.) is shown in the figure 2.

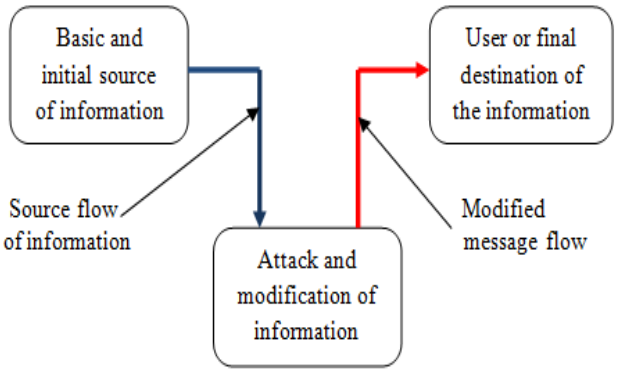


*Fig.2. Modified message flow*

The next type of attack involves learning about the content of the information being transmitted, its secrecy and confidentiality. In this way, an unauthorized person who does not have the right of access, through interception, gets access to the content of the information. With the help of appropriate software and programs, a third party in the attack can illegally copy the transmitted information. In this case, the searcher or the final destination receives the information without change, but also without knowing that the attacker also received the same information. An example could be the sending of state confidential information, a conceptual solution to a traffic problem, or the discovery of a new medicine in healthcare, etc. Based on the information obtained through interception, an unauthorized person can use it for his own needs. Interception of information is shown in the figure 3.

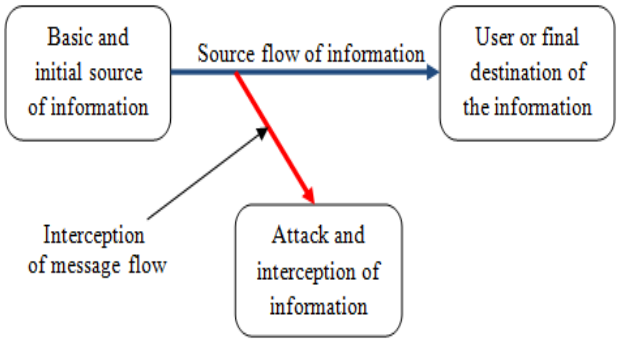


*Fig.3. Interception of message flow*

The next type of attack refers to information fabrication, where an unauthorized person creates false messages within a possible information stream. An example can be identity theft of a certain person and impersonation by sending messages that have wrong information or modifying some messages in the communication of interested parties. Fabrication of information where the requester or the final destination believes that the message was sent from the correct address is shown in the figure 4.

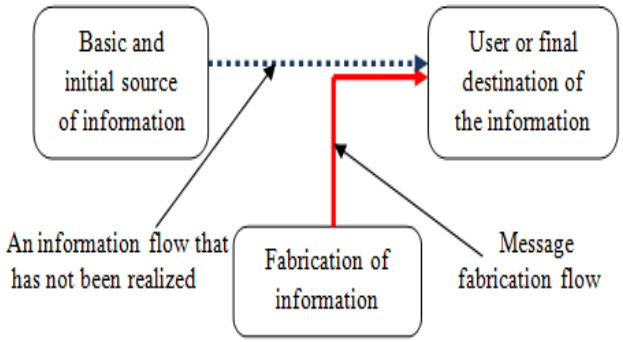


*Fig.4. Fabricated message flow*

## 3. PROTECTION MECHANISMS IN ELECTRONIC BUSINESS

Cryptography is the science of secret writing where it has the basic task of securing information from potential attackers. At first, cryptographic techniques allow the sender to mask the data so that if someone tries to intercept it, they don't get any information they can misuse. This implies that the recipient is able to extract the original data sent that has been masked by the sender.

Block encryption means when a message to be encrypted is processed in blocks consisting of bits. For example if the message consists of 64, each one is broken separately and we have blocks of 64 bits. After breaking the message, each block is encrypted independently. When one block is encrypted, a one-to-one mapping is performed and one bit block of the plaintext is mapped into a bit block of the encrypted text. With this mapping, there is a different output for each input. Block encryption allows a large number of mappings and also a large number of combinations that can occur . Each mapping represents one key. If the sender and recipient of the message know a certain mapping, they have the ability to encrypt and decrypt the messages they exchange with each other. For block encryption in this case, there are a large number of combinations. It means that the sender and receiver must have a scheme with as many possible mappings.

Other block cipher algorithms represent standards known by the following names:

- DES (Data Encryption Standard);
- 3DES (3 x Data Encryption Standard) i
- AES (Advanced Encryption Standard).

These operating standards use functions rather than predefined tables as in block ciphers. A string of bits is used as a key in the algorithm. The DES algorithm uses 64-bit blocks with 56-bit keys, while AES uses 128-bit blocks with keys of 128, 192, and 256 bits in length. Table mapping and the number of iterations within the algorithm is the key.

Due to the large number of blocks in the messages that are forwarded and that are too long, a new mechanism has been devised that implies the use of an initial vector for the first block to be encrypted. Chain encryption of blocks is the next protection mechanism and the main characteristics are [7]:

- When encrypting a message, the sender generates a random sequence of bits called the initial vector which is sent as plain text;
- For the first block of encryption, an initial vector is used to calculate the first block of plain text, then the results are passed through the block encryption algorithm and, based on the above, a corresponding block of encrypted text is obtained. The next step involves sending the encrypted block to the recipient;
- The recipient receives a block consisting of an initial vector and an encrypted block of text that is decrypted and can receive the original source text.

## 4. THE STRONGEST PROTECTION MECHANISM – BLOCKCHAIN TECHNOLOGY

Now the question arises, why is block chain technology the strongest cyber security mechanism in e-business? The answer represents and includes the scalability, security and decentralization of (Figure 5).

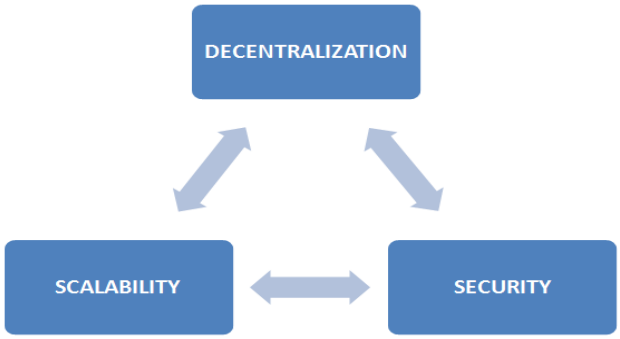


*Fig.5. Basic components of blockchain*

Decentralization allows remote nodes to manage the network peer-to-peer instead of central control. In addition to the above, decentralization enables each transaction (message exchange) to be validated by more than half of the nodes in the network. There is a possibility of expanding the network where a large number of nodes increases security and at the same time the number of transactions can be reduced. The solution to expanding the network with new nodes is in another basic component called scalability. Scalability has the ability to accommodate a larger number of new applications as well as new transactions without affecting the bandwidth of the entire block chain technology. The network can continuously grow and support new transactions. And finally, security in the block chain network is guaranteed because during a cyber attack, an attacker cannot take over more than half of the nodes that function independently on the basis of

decentralization.

For ease of understanding, a six-step process is described below and is presented in figure 6. In the first step, a transaction is initiated by the user or device. The second step is tasked with publishing the transaction to the blockchain network. The following third step executes the consensus using the protocol and at the same time the validation of the initiated transaction is performed. In the fourth step after the transaction is validated, the transaction is grouped with other transactions to form a new block in the main ledger. After that, in the fifth step, a new block is created, which is cryptographically linked to the previous block. In the sixth step, it is confirmed that the transaction that was initiated has been completed.

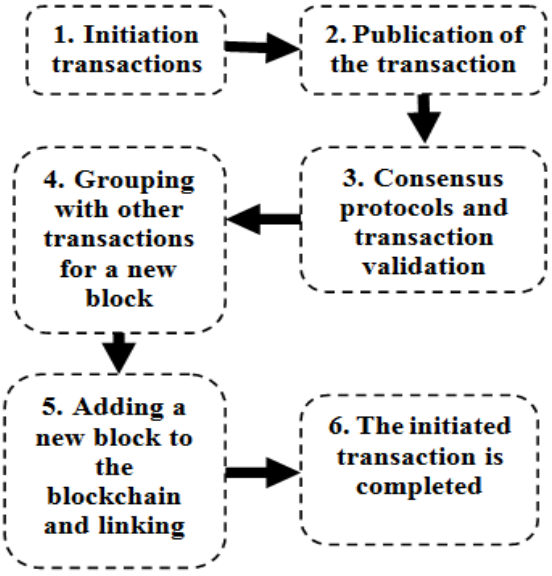


*Fig.6. Data protection procedure*

## 5. CONCLUSION

In the recent past, blockchain technology was only applied in the banking sector with cryptocurrencies. Today, the innovative blockchain technology can be applied in all areas of electronic business. A large number of processes in railway traffic and transport take place via computers and the Internet.

In this paper, the available mechanisms for protecting and increasing cyber security in all processes of electronic business are analyzed. Railway companies are increasingly applying technologies and therefore have to secure and insure their personal property as well as the property of partners and potential users. The transparency of the application of technologies should be as accessible as possible and explained in detail to people so that they themselves can introduce the advantages and that their participation in the processes of electronic business is completely safe. Block chain technology as well as its application secures business from cyber attacks in the railway company. The willingness of employees to accept innovative technology can be improved by organizing seminars and teaching so that they can directly communicate the possibility of applying electronic business from their homes in a safe and secure way.

## REFERENCES

[1] Bozidar Radenkovic et al , *E-business* , FON Belgrad, 2015

[2] Nebojša Backović i ostali , *Elektronsko poslovanje i Internet marketing*, Planeta print-Beograd, Leposavić,2009

[3] Pavlović Z. G., "Technologies of electronic business in traffic," *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2022, pp. 1-4, doi: 10.1109/INFOTEH53737.2022.9751297. https://ieeexplore.ieee.org/document/9751297

[4] Z. G. Pavlović, "Development Of Models Of Smart Intersections In Urban Areas Based On IoT Technologies," *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2022, pp. 1-4, doi: 10.1109/INFOTEH53737.2022.9751263. https://ieeexplore.ieee.org/document/9751263

[5] Z. Pavlović, *User'S Ability To Use Internet Tecnologies In Transport*, 7th International Conference ''Towards A Humane City''Environmentally Friendly Mobility, Serbia, Novi Sad 6th and 7th December 2019, pp 207-213, https://www.dropbox.com/s/95zjnjm3npxzzfr/Conference%20proceedings%20TAHC_2019.pdf?dl=0

[6] Radičević, V., Pavlović, Z. **G.,** & Nikolić, D. (2021, 10 15). *Analiza mobilnih tehnologija i aplikacija.* (Z. Čekerevac, Ur.) FBIM Transactions, 9(2), 94-101. doi:10.12709/fbim.09.09.02.10 ; https://www.meste.org/fbim/FBIM_2_2021/18_10.pdf

[7] Kurose, J. F., Ross, K. W. *Computer Networking: A Top-Down Approach* (7th Ed.).Manhattan: Addison-Wesley,2018.