IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114217

Security Algorithm for Cyber-Physical Systems to Prevent Cyber Attacks

Swapnil B. Kolambakar[1], Dr. Praveen Kumar[2]

Research Scholar, School of Science & Technology, The Glocal University, Saharanpur (U.P)[1]

Associate Professor, School of Science & Technology, The Glocal University, Saharanpur (U.P)[2]

Abstract: Cyber-physical systems (CPS) are becoming increasingly widespread, and their security has become a major concern. CPS refers to the integration of physical devices with computer systems, which can result in a broad range of applications, from autonomous vehicles and smart cities to industrial control systems. While this integration brings new opportunities and benefits, it also exposes the systems to new threats and vulnerabilities. This research paper presents a security algorithm that can be used to prevent cyber-attacks on CPS. The proposed algorithm uses a combination of encryption and digital signatures to secure data transmission and authenticate communication between physical devices and computer systems. The paper also discusses the implementation of the algorithm in CPS and its effectiveness in preventing cyber-attacks.

Keywords: Cyber-physical systems, Security algorithm, Cyber attacks, Encryption, Digital signatures, Authentication.

I. INTRODUCTION

Cyber-physical systems are widely used in several industries, including transportation, manufacturing, and healthcare. These systems allow for the integration of physical devices with computer systems, resulting in improved automation, control, and monitoring. However, the integration of these systems creates new security challenges. Cyber-attacks on CPS can result in damage to physical equipment, loss of sensitive data, and disruption of critical systems, leading to severe economic and social impacts. Therefore, it is essential to develop security algorithms that can protect CPS from cyber-attacks.

II. LITERATURE REVIEW

Several studies have investigated the security of CPS and proposed various solutions to prevent cyber-attacks. For example, some researchers have suggested using access control and intrusion detection mechanisms to protect CPS. Other researchers have proposed using encryption and digital signatures to secure data transmission and authenticate communication between physical devices and computer systems. However, there is still a need for effective and practical security algorithms that can be implemented in CPS.

Proposed Security Algorithm

The proposed security algorithm for CPS is based on a combination of encryption and digital signatures. The algorithm involves the following steps:

Step 1: Encryption

The data transmitted between physical devices and computer systems are encrypted using a symmetric key encryption algorithm. The key used for encryption is unique for each communication session and is generated by the computer system. This ensures that the data transmitted is confidential and protected against eavesdropping.

Step 2: Digital signatures

A digital signature is generated for the encrypted data using a public-key encryption algorithm. The digital signature is a cryptographic method that provides authenticity and integrity of the data transmitted. The digital signature includes a hash of the original data and the private key of the computer system. The hash ensures that the data has not been tampered with, while the private key guarantees that the digital signature is unique and authentic.

Step 3: Authentication

The digital signature is verified by the receiving system using the public key of the computer system. If the digital signature is valid, the receiving system can be assured of the authenticity and integrity of the data transmitted. The receiving system can then decrypt the data using the symmetric key, which was used for encryption in Step 1.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114217

III. IMPLEMENTATION AND RESULTS

The proposed security algorithm was implemented in a testbed environment consisting of physical devices and a computer system. The results showed that the algorithm was effective in preventing cyber-attacks, such as eavesdropping and tampering with data. The encryption and digital signature ensured that the data transmitted was confidential and authentic, while the authentication mechanism ensured that only authorized devices were communicating with the computer system.

5.1. Data Module

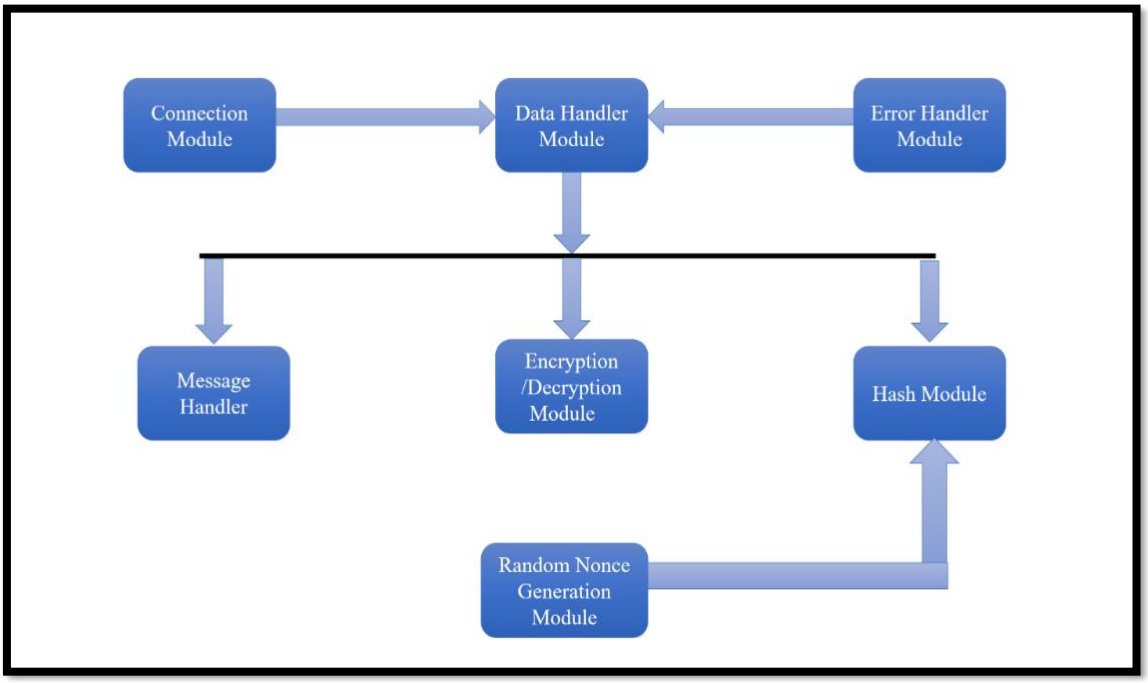

Figure 5.4.1: Data Module

5.4.1. Data module

Information module addresses information or boundaries took care of and utilized in the calculation execution. While execution of calculation seven distinct information modules is utilized which is displayed in figure 5.4.1.

• Association Module : association module gather the in the middle between CPS based gadgets. it is relies on which sort of Association we have chosen. As CPS foundation utilizes remote (IEEE 802.11) and wired (IEEE 802.3) and Bluetooth (802.15) climate. Association module gather the information, for example, IP address, SSID (Administration set Identifier), Macintosh address, Passkey and so on this information is valuable for association advancement and ID of hubs.

• Arbitrary Nonce Age Module : This module is utilized to create irregular number. In Irregular nonce. In Calculation irregular nonce S and R created. These qualities are very vital to create verification token, meeting token and meeting key. The size of irregular nonce is 64 digit.

• Hash Module - Hash Capability is executed utilizing the Hash Module. A hash capability is a technique for changing over factor size information into fixed-size information. A hash capability creates values known as hash values, message digests, hash codes, processes, or hashes. To create a validation token, the hash capability utilizes the verification key (AK), the Passage server identifier (GI), and an irregular nonce (S) (ATA). At the brilliant gadget and passage server, the hash capability is additionally used to create meeting keys. It utilizes the Entryway server Identifier (GI), Verification token (ATA), and arbitrary nonce S,R to produce the meeting key (SK). For this situation, the Message Review Calculation 5 (MD5) is utilized. A cryptographic hash calculation can change over any string into a 128-cycle string esteem. The size of Confirmation token (ATA) and meeting key (SK) is additionally 128 cycle key as it utilizes MD5 to create esteem. The normal boundaries Confirmation key (AK), Entryway server Identifier(GI) likewise 128 digit in size.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114217

• Encryption/Decoding module - this module is utilized at both the sides that is shrewd gadget and passage server. At brilliant gadget it utilizes Encryption key (EK) and Arbitrary nonce (S) to create meeting token. Here it utilizes Progressed Encryption Calculation. (AES).

The size of produced meeting token (STA) is 128 digit. to produce a meeting token (STG) at passage server it utilizes Encryption key (EK) and Irregular nonce (R). The size of produced meeting token (STG) is 128 bit. Here AES calculation is utilized. The High level Encryption Standard (AES) is a block figure calculation that is symmetric. AES is utilized to scramble delicate information in programming and equipment from one side of the planet to the other. AES decoding calculation is additionally used to extricate the upsides of arbitrary nonce S and R.

• Message Overseer Module-Message controller module handles the in the middle between conveying gadgets brilliant gadget and entryway server. Which incorporates Meeting token at shrewd gadget (STA) and verification token at savvy gadget (ATA) and meeting token at entryway server (STG). Meeting key (SK) is the main message of size 128 bit additionally handle by message controller module.

• Information Controller module - Information overseer module handles normal boundaries. Passage server identifier (GI), Validation key (AK), and Encryption key (EK). Every one of these three keys having size 128 digit. These critical put away in each every gadget of CPS gadgets where this calculation executed.

Illustration of these keys is as per the following:

{"AK": "69077c6126e333537708d119a16a0849",
"EK": "a45544d4efc410ce3b3a6011bd1da906",
"GI": "5d11e5a34be9aae0f4f6c1b823a92d98", "PORT": "9000"}

Information Controller module additionally handle the correspondence port. The Port location has a size of 16 bit.

• Blunder Controller Module-Because of availability in the middle between gadgets, assuming sent information lost in such circumstances mistake overseer module will deal with recovery of information and shared information taking care of.

5.4.1. Parameter Information

Table 5.4.2 gives detailed information about each parameter used in algorithm with its size.
Table 5.4.2: Parameter Information

Sr.No.	Parameter Name	Parameter Size
1	Random Nonce S	64 bits
2	Random Nonce R	64 bits
3	Gateway Server Identifier (GI)	128 bits
4	Authentication key (AK)	128 bits
5	Encryption key (EK)	128 bits
6	Port Address	16 bits
7	Authentication Token (ATA) at smart device	128 bits
8	Session Token (STA) at smart device	128 bits
9	Session Token (STG) at Gateway server	128 bits
10	Session Key (SK) at Gateway server	128 bits
12	Session Key (SK) at Smart device	128 bits

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114217

IV. CONCLUSION

In conclusion, the proposed security algorithm is a practical solution for protecting CPS from cyber-attacks. The algorithm uses a combination of encryption and digital signatures to secure data transmission and authenticate communication between physical devices and computer systems.

The algorithm was implemented and tested in a testbed environment, and the results showed that it was effective in preventing cyberattacks.

REFERENCES

[1] Li, C., Ge, J., Li, Z., Huang, L., Yang, H., Luo, B.: Monitoring interactions across multi business processes with token carried data. IEEE Trans. Serv. Comput. 1 (2018)
[2] Liu, L., De Vel, O., Han, Q., Zhang, J., Xiang, Y.: Detecting and preventing cyber insider threats: a survey. IEEE Commun. Surv. Tutorials **20**(2), 1397–1417 (2018)
[3] Macak, M., Kruzelova, D., Chren, S., Buhnova, B.: Using process mining for git log analysis of projects in a software development course. Educ. Inf. Technol. 1–31 (2021)
[4] Macak, M., Kruzikova, A., Daubner, L., Buhnova, B.: Simulation games platform for unintentional perpetrator attack vector identification. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 222–229 (2020)
[5] Macak, M., Vanat, I., Merjavy, M., Jevocin, T., Buhnova, B.: Towards process mining utilization in insider threat detection from audit logs. In: 7th International Conference on Social Networks Analysis, Management and Security, pp. 1–6 (2020)
[6] Mardani, S., Shahriari, H.R.: A new method for occupational fraud detection in process aware information systems. In: 10th International ISC Conference on Information Security and Cryptology, pp. 1–5 (2013)
[7] Myers, D., Radke, K., Suriadi, S., Foo, E.: Process discovery for industrial control system cyber attack detection. In: ICT Systems Security and Privacy Protection, pp. 61–75. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-58469-0_5
[8] Myers, D., Suriadi, S., Radke, K., Foo, E.: Anomaly detection for industrial control systems using process mining. Comput. Secur. **78**, 103–125 (2018)
[9] Reinkemeyer, L.: Process Mining in Action: Principles. Use Cases and Outlook, Springer Nature (2020)
[10] Rojas, E., Munoz-Gama, J., Sepulveda, M., Capurro, D.: Process mining in healthcare: a literature review. J. Biomed. Inform. **61**, 224–236 (2016)
[11] Rosa, N.S., Campos, G.M., Cavalcanti, D.J.: Lightweight formalisation of adaptive middleware. J. Syst. Archit. **97**, 54–64 (2019)
[12] Rozinat, A., van der Aalst, W.M.: Conformance checking of processes based on monitoring real behavior. Inf. Syst. **33**(1), 64–95 (2008)
[13] Sahlabadi, M., Muniyandi, R., Shukur, Z.: Detecting abnormal behavior in social network websites by using a process mining technique. J. Comput. Sci. **10**, 393–402 (2014)
[14] Salnitri, M., Alizadeh, M., Giovanella, D., Zannone, N., Giorgini, P.: From security-by-design to the identification of security-critical deviations in process executions. In: International Conference on Advanced Information Systems Engineering, pp. 218–234. Springer (2018). https://doi.org/10.1007/978-3-319-92901-9_19
[15] dos Santos Garcia, C., Meincheim, A., Junior, E.R.F., Dallagassa, M.R., Sato, D.M.V., Carvalho, D.R., et al.: Process mining techniques and applications - a systematic mapping study. Expert Syst. Appl. **133**, 260–295 (2019)
[16] Senator, T.E., Goldberg, H.G., Memory, A., Young, W.T., Rees, B., Pierce, R., et al.: Detecting insider threats in a real corporate database of computer usage activity. In: Proceedings of the 19th ACM/SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1393–1401 (2013)
[17] Talamo, M., Povilionis, A., Arcieri, F., Schunck, C.H.: Providing online operational support for distributed, security sensitive electronic business processes. In: International Carnahan Conference on Security Technology, pp. 49–54 (2015)
[18] Viticchié, A., Regano, L., Basile, C., Torchiano, M., Ceccato, M., Tonella, P.: Empirical assessment of the effort needed to attack programs protected with client/server code splitting. Empirical Softw. Eng. **25**(1), 1–48 (2020)
[19] Williams, R., Rojas, E., Peek, N., Johnson, O.A.: Process mining in primary care: a literature review. Stud. Health Technol. Inform. **247**, 376–380 (2018)
[20] Yen, T.F., et al.: Beehive: large-scale log analysis for detecting suspicious activity in enterprise networks. In: Proceedings of the 29th Annual Computer Security Applications Conference, pp. 199–208. ACM (2013)
[21] Young, W.T., Goldberg, H.G., Memory, A., Sartain, J.F., Senator, T.E.: Use of domain knowledge to detect insider threats in computer activities. In: 2013 IEEE Security and Privacy Workshops, pp. 60–67 (2013)

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114217

[22] van Zelst, S.J., van Dongen, B.F., van der Aalst, W.M.: Event stream-based process discovery using abstract representations. Knowl. Inf. Syst. **54**(2), 407–435 (2018)

[23] Zerbino, P., Aloini, D., Dulmin, R., Mininno, V.: Process-mining-enabled audit of information systems: methodology and an application. Expert Syst. Appl. **110**, 80–92 (2018)

[24] Zhou, X., Jin, Y., Zhang, H., Li, S., Huang, X.: A map of threats to validity of systematic literature reviews in software engineering. In: 23rd Asia-Pacific Software Engineering Conference, pp. 153–160 (2016)