ADVANCED MULTIMEDIA PLATFORM BASED ON BIG DATA AND ARTIFICIAL INTELLIGENCE IMPROVING CYBERSECURITY

Alessandro Massaro[1]*, Gaetano Panarosa[1], Nicola Savino[1],
Simone Buonopane[2] and Angelo Galiano[1]

[1]Dyrecta Lab, IT Research Laboratory, via Vescovo Simplicio, 45,
70014 Conversano (BA), Italy
[2]Spacertron srl, Via degli Abruzzi 13/a, Milano, Italy

ABSTRACT

The proposed work describes the design of a multimedia platform managing users and implementing cybersecurity. The paper describes in details the use cases of the whole platform embedding Big Data and artificial intelligence (AI) engine predicting network attacks. The platform has been tested by Tree Ensemble algorithm classifying and predicting anomalous server logs of possible attacks. The data logs are collected in Cassandra Big Data System enabling the AI training model. The work has been developed within the framework of a research industry project.

KEYWORDS

Cybersecurity, Artificial Intelligence, Attacks Prediction, Cassandra Big Data.

1. INTRODUCTION

Data security is an important research topic in industry research [1]. Concerning this topic, multimedia platforms could be easily attacked in al cyberspace environments. Multimedia platforms are commonly used for e-learning [2] managing different multimedia contents such as text, audio, images, animation and video [3]-[6]. The management criteria of multimedia files and the computational cost of the relative transmission will therefore depend on how they are structured and unpacked and on the security measures (firewall, encryption, identification/authorization accesses, etc.). Regarding the security of data travelling online, important studies have been carried out on the risks associated with the control of industrial systems [7]. These risks mainly concern product protection, production qualities, brand reputation, and human life safety, and increased with the advent of Industry 4.0 technologies, mobile computing, and Internet of Things (IoT) technologies [7]. Specifically, in the IoT area, information security is associated with multiple levels such as the server/provider level, the network level and the user level [8]. The violations at the different levels can concern [9]-[13]:

- listening of communication channels;

- stopping operations/functions of operating systems using radio signals applied to broadcasting devices;

- interception with data manipulation;

- use of data;

- data and information connection and use;

- duplication of data by third parties;

- obtaining customer data and sending false data to monitoring centers.

About data security intervention in the machine to machine (M2M) field [14] can be adopted and optimized the following techniques [15]-[22]:

- Privacy Enhancing Technology (PET);

-Virtual Private Network (VPN);

- Transport Layer Security (TLS);

- Onion routing;

- E-Awareness model;

- Cryptography algorithm;

- Public Private Partnership (PPP);

- Markov process;

-Authentication, Authorization and Accounting (AAA) services;

- Traffic management and fault tolerance technique;

- Localized cooperative access, stabilization algorithm;

- Symmetric Algorithm, Hash algorithm.

These technologies can be adopted in different application fields such as [22]:

- attacks on mobile devices;

- cyber terrorism;

-vulnerabilities of web platforms used for managing multimedia content;

- steganography techniques;

-adaptive defence based on the intelligent use of information for a long-term capacity building strategy;

- cryptographic algorithms.

Of particular scientific interest could be the management of data security in Big Data systems [23],[24]. All the mentioned security techniques and approaches can be applied for platforms

managing multimedia data by ensuring a secure cloud infrastructure. The paper is organized as follows:

-is provided a design of the prototype hardware architecture including use cases of the platform describing system actors and related functions;

-is checked the system attack detection by a Tree Ensemble algorithm designed to read and process data log information;

-is described the configuration and the implementation of Cassandra Big Data system containing server data logs used for attack detection.

2. MAIN SYSTEM ARCHITECTURE

The prototype multimedia platform used for experimentation is sketched by the system architecture of Fig. 1, structured by the following elements:

- Access Switch Layer2+ 10/100/1000 Mbps / Core Switch Layer2+ 10/100/1000 Mbps: this is the hardware connecting each rack on a computer network by using a packet switching to receive and forward data at the network layer 3 of ISO/OSI standard model.

- IPS/IDS/FW/DNS: two firewalls installed after the access switch layer which works in an exogen modality detecting and preventing some intrusions or attacks from external clients.

- There are two couple of endogen firewalls too, identical to the exogen firewalls but inserted after a hardware VPN server, which purpose is to ensure a cleaned connection from any type of malicious action to the system.

- Notification Server: this hardware component transmits a message to the system administrator when there are some problems about diagnostic or when the firewalls detect an intrusion or a system attack.

- Registration Server: this hardware component stores all events about the state of the system.

- Syslog Server: this hardware component generates logs and stores them. Each message is labelled with a facility code, indicating to the software the type of generated message, and assign to it a severity level.

- NAS Server: the Network - Attached Storage (NAS) Server is a file-level computer data storage server connected to a computer network specialized for serving files either by its hardware, software or configuration.

- VPN Server: this component allows the connection of the rack to a computer network through a VPN (Virtual Private Network), improving the security level of the system.

- SIP Server: the SIP Server (Session Initiation Protocol) is a signaling protocol used for manage real-time sessions of voice, video and messaging applications.

- Antivirus: this component is a computer program used to prevent, detect and remove malware or any type of malicious item which escaped from the detection of the firewall.

- TMMS /APP: this component has the purpose to manage Mobile Devices (MDM) and Mobile Apps (MAM).
- Chat Server: this is a server managing the chat services.
- PhoneBook Server: this is a server managing contacts for VOIP services, chat services, and mail services.
- Mail Server: this is a server managing mail services.
- System SMS App Sw Server: this is a server managing SMS services.
- System NMS App Sw Server: the purpose of this hardware component is that to manage the devices on the network.
- SRV Front End Web App: a dedicated server for web applications of the system.
- SRV Core Process: is a server dedicated for the elaboration and processing of services.
- SRV Database: is a dedicated server for storage and management any type of DBMS (Data Base Management System).

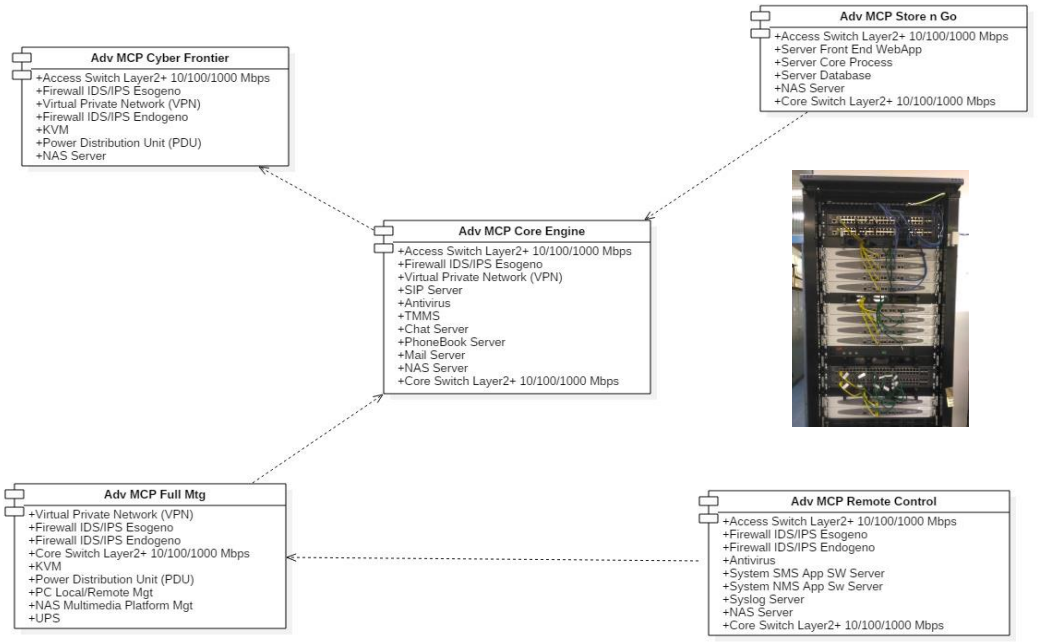

Figure 1. Architecture of the whole server system (inset: hardware components used for the testing).

The Access Switch Layer is the part of the backbone network linking the modules through a VPN connection. Each switch is connected directly to a VPN Server to improve the platform security. The Switch backbone uses a star topology with one switch allocated in the Adv MCP Core Engine (see Fig. 1). This rack or module is the core of the backbone network having a maximum bandwidth of 1000/Mbps. The internet connection used for tests has 100Mbps speed.

3. SYSTEM USE CASE

In this paragraph are listed the main use cases of the architecture shown in Fig. 1 describe the whole multimedia platform.

Use case 1 (see Fig. 2)

Actors: the actor, called User, develops the main activities such as platform management and User Operations.

Platform Management: managing of the Address Book (Rubric), necessary to save the various contact details of other users (email address for Mail, the Chat nickname, telephone number for Voip) and Services (Streaming, Mail, Chat, Voip and File Sharing).

Operations User Operations: this function includes registration on the web platform and Login. The use case is extended by the Log in Account Management, which includes the operations of modifying and deleting the personal account data.

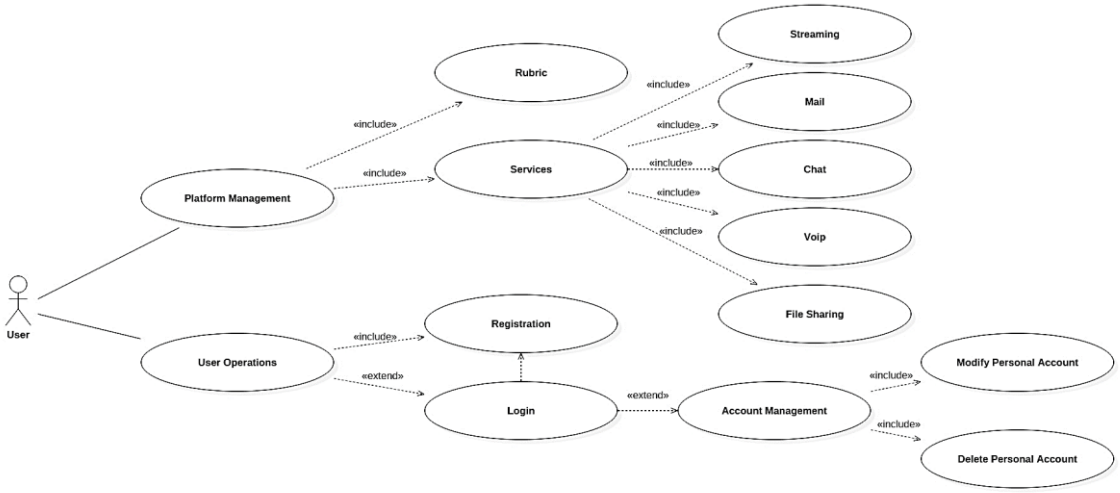

Figure 2. Architecture of the proposed architecture (use case 1).

Use case 2 (see Fig. 3)

Actors: the actor, called Admin is the web platform administrator.

User Account Operation: the Admin, performs operations on User Accounts, accesses all the platform data and manipulates them into the Big Data system.

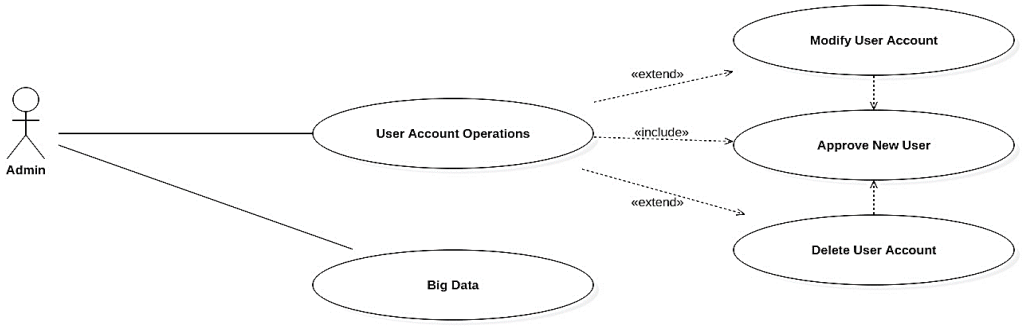

Figure 3. Architecture of the proposed architecture (use case 2).

Use case 3 (see Fig. 4)

Actors and operations: the SuperAdmin through an Artificial Intelligence Engine (AI Engine) accesses, interrogates and manipulates the data stored into the Big Data system, carrying out operations and tasks that the Administrator cannot perform.

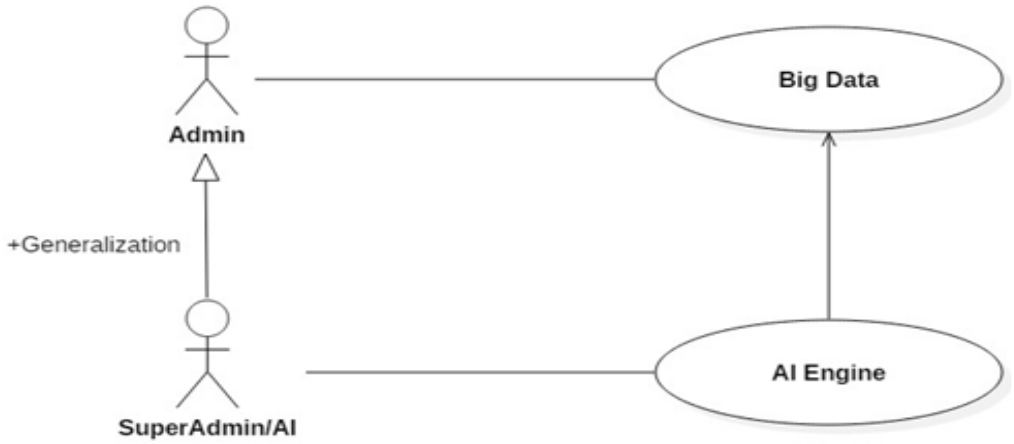

Figure 4. Architecture of the proposed architecture (use case 2).

Use case 4 (see Fig. 5)

Actors and operations: Fig. 5 illustrates the Admin SuperAsmin/AI and User relationships managing all the platform information and operations.

Figure 5. Architecture of the proposed architecture (use case 4).

4. DATA MINING APPLICATION AND BIG DATA STORAGE

In this section is discussed the designed and implemented Konstanz Information Miner (KNIME) workflow [25]-[33] predicting server attacks. The adopted data mining algorithm is the Ensemble method, which combines several decision trees to produce better predictive performance using a single decision tree. The testing workflow is illustrated in Fig. 5. It is structured by connecting the following blocks:

- "File Reader": node reading log data extracted from server machine (the input data are the alert log and the Syslog containing more information about admin, IP address and subnet mask, ports, etc.);
- "Partitioning": the input table is split into the two partitions of train and testing dataset; the two partitions are available at the two output ports;
- "Tree Ensemble Learner": this block learns an ensemble of decision trees such as random forest variants).
- "Tree Ensemble Predictor": this block predicts patterns according to an aggregation of the predictions of the individual trees in a random forest model.
- "Column Filter": this node takes a data table and returns a filtered data table with only the selected columns;
- "CSV writer": this node writes the output results into a csv file;

- "Scorer": this block provides the performance of the adopted model.

In Fig. 7 is illustrated the data input of the workflow of Fig. 6: the log protocol is constructed by the fields timestamp (time arrival of the log), request type (request type such as port access request), message (returned message following the request), IP request (origin Internet Protocol), IP arrival (destination IP), IP request port (origin port), IP Arrival Port (destination port corresponding the arrival IP). The Request type field is the labelled attribute for the prediction outputs. The input table contains 120 log records structured in the previously described protocol. Each record arrives after a period. The message, Ip Arrival, IP Request Port and the IP Arrival Port define the information pattern to analyze, in order to distinguish an attack from a normal system log (output of the Tree Ensamble algorithm processing all the information sequences). The algorithm provides an alerting if all the four fields present an anomaly, thus decreasing the calculus probability error. In Fig. 8 is illustrated the input table of the workflow of Fig. 6. A good model performance is checked observing a good percentage of confidence values (70% as shown in Fig. 9).

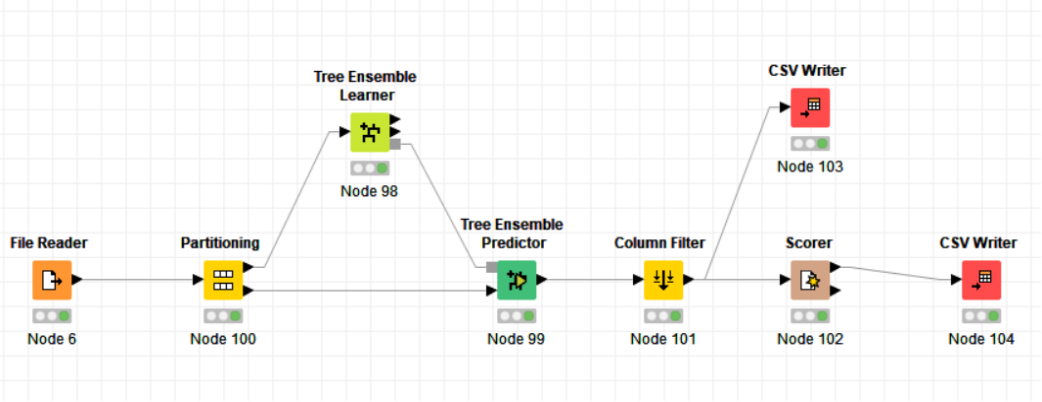

Figure 6. Tree Ensemble workflow predicting server attacks.

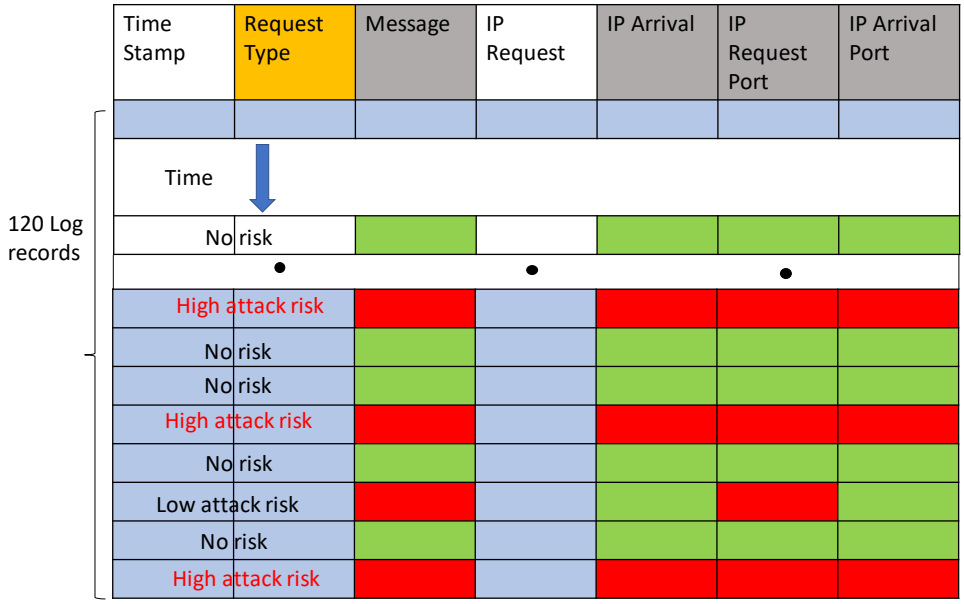

Figure 7. Log matrix at the input of the Tree Ensemble network, and risk estimation criterium.

Col0	Col1	Col4	Prediction (Col1)	Prediction (Col1) (Confidence)
05/31/19-21:58:37.099780	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9900000095367432
05/31/19-22:03:36.175308	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9900000095367432
05/31/19-22:03:44.504569	(http_inspect) DOUBLE DECODING ATTACK	147.75.102.200	(http_inspect) DOUBLE DECODING ATTACK	0.9599999785423279
05/31/19-22:08:37.305918	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9599999785423279
05/31/19-22:11:23.008016	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9100000262260437
05/31/19-22:11:29.168257	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9700000286102295
05/31/19-22:11:32.548987	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9700000286102295
05/31/19-22:11:40.934191	(http_inspect) PROTOCOL-OTHER HTTP server response before client request	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9100000262260437
02/07/2018 15:44	System started counting down to shutdown.	admin	System started counting down to reboot.	0.2800000011920929
25/02/2018 12:52	IP address [169.254.215.177] and subnet mask [255.255.0.0] were assigned to the DHCP client on [LAN 2].	SYSTEM	IP address [169.254.215.177] and subnet mask [255.255.0.0] were assigned to the DHCP client on [LAN 2].	0.4000000059604645
15/09/2017 10:01	System started to boot up.	SYSTEM	IP address [169.254.215.177] and subnet mask [255.255.0.0] were assigned to the DHCP client on [LAN 2].	0.4000000059604645
05/31/19-22:17:35.286915	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9800000190734863
05/31/19-22:21:27.300013	(POP) Unknown POP3 response	178.23.173.228	(POP) Unknown POP3 response	0.6399999856948853
05/31/19-22:21:47.865102	(POP) Unknown POP3 command	82.57.200.129	(POP) Unknown POP3 command	0.8899999856948853
06/02/19-12:30:35.088305	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9700000286102295
06/03/19-12:45:01.478661	(POP) Unknown POP3 response	178.23.173.228	(POP) Unknown POP3 response	0.6000000238418579
06/03/19-12:49:23.993279	(POP) Unknown POP3 response	178.23.173.228	(POP) Unknown POP3 response	0.6399999856948853
06/03/19-12:49:24.073035	(POP) Unknown POP3 command	62.211.72.20	(POP) Unknown POP3 command	0.9700000286102295
06/03/19-12:49:27.800176	(http_inspect) DOUBLE DECODING ATTACK	51.89.9.252	(http_inspect) DOUBLE DECODING ATTACK	0.8799999952316284
06/03/19-12:49:35.334287	(http_inspect) PROTOCOL-OTHER HTTP server response before client request	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9700000286102295
06/03/19-12:49:35.334287	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	178.23.173.228	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	0.9700000286102295
06/03/19-12:49:50.474226	(POP) Unknown POP3 command	62.211.72.20	(POP) Unknown POP3 command	0.9100000262260437
06/03/19-19:45:04.508293	(spp_sip) Content length mismatch	178.23.173.228	(spp_sip) Content length mismatch	0.28999999165534973
06/04/19-10:25:41.883129	(http_inspect) DOUBLE DECODING ATTACK	51.89.9.251	(http_inspect) DOUBLE DECODING ATTACK	0.9700000286102295

Figure 8. Output of the worflow of Fig. 6 predicting attacks.

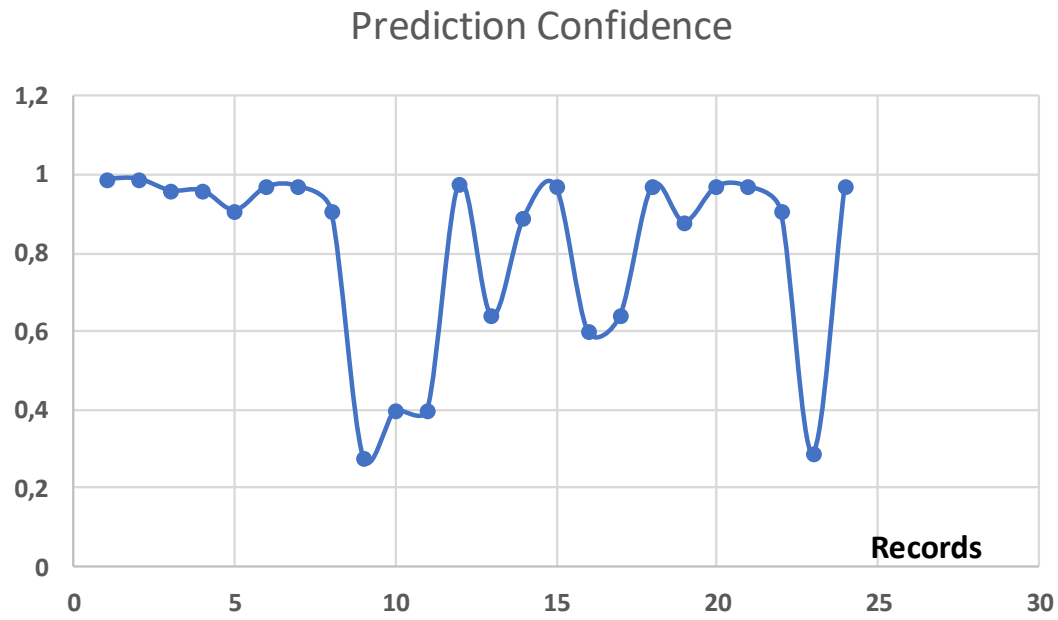

Figure 9. Prediction confidence.

The algorithm analyses simultaneously the alert log (dangerous log) and the Syslog (not dangerous log) by classifying the new registered log. The workflow will detect the normal log patterns by classifying anomalous ones.

The discussed workflow can be embedded into an object container executing on the server operating system. The risk output matrix is stored into the Cassandra Big Data System thus optimizing the training dataset and consecutively the data processing model. A good performance for single node write, delete and read operation is found for Cassandra Big Data System if compared the computational costs with other big data systems such as HBase and MongoDB [33]. The proposed Big Data system is suitable for Industry 4.0 implementation [34]. In appendix are reported main scripts of Cassandra configuration. Below are reported some Cassandra screenshots proving the correct Big Data configuration.

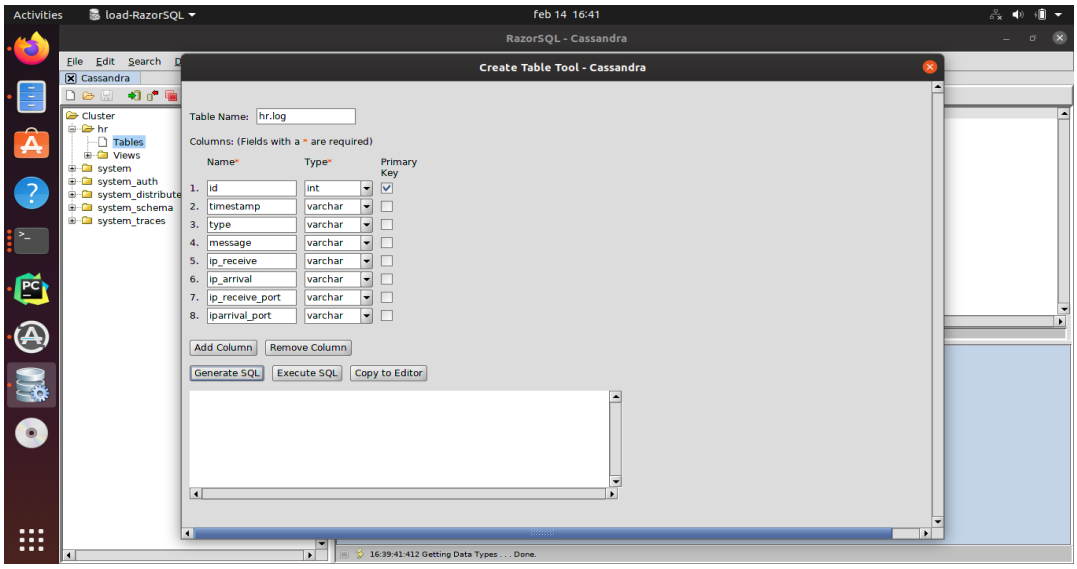

Figure 10. Cassandra table creation: the table is structured to contain records of Fig. 8.

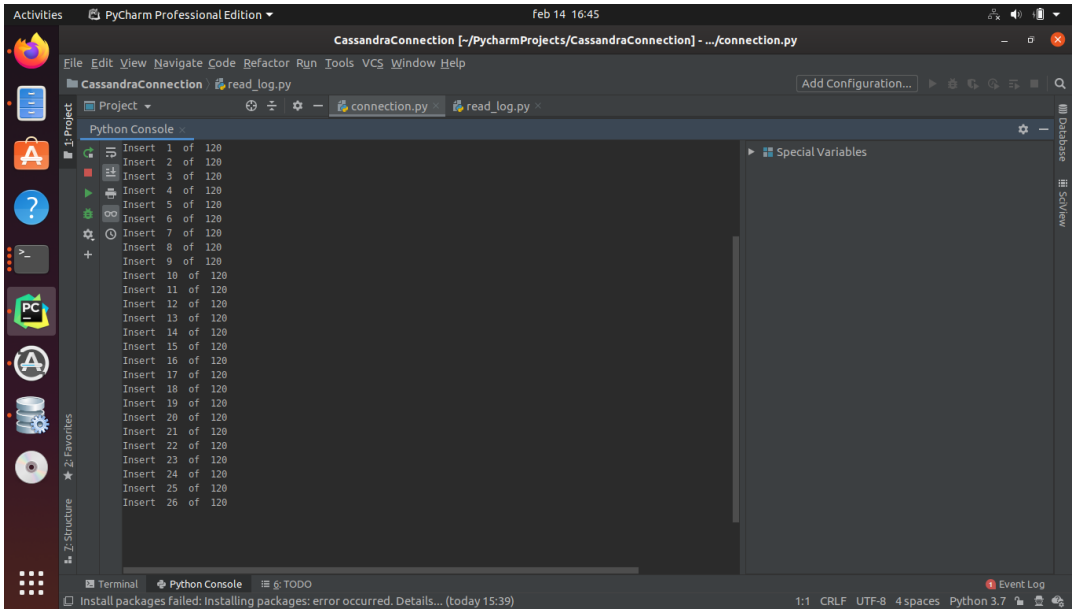

Figure 11. Cassandra connection check and writing of testing records.

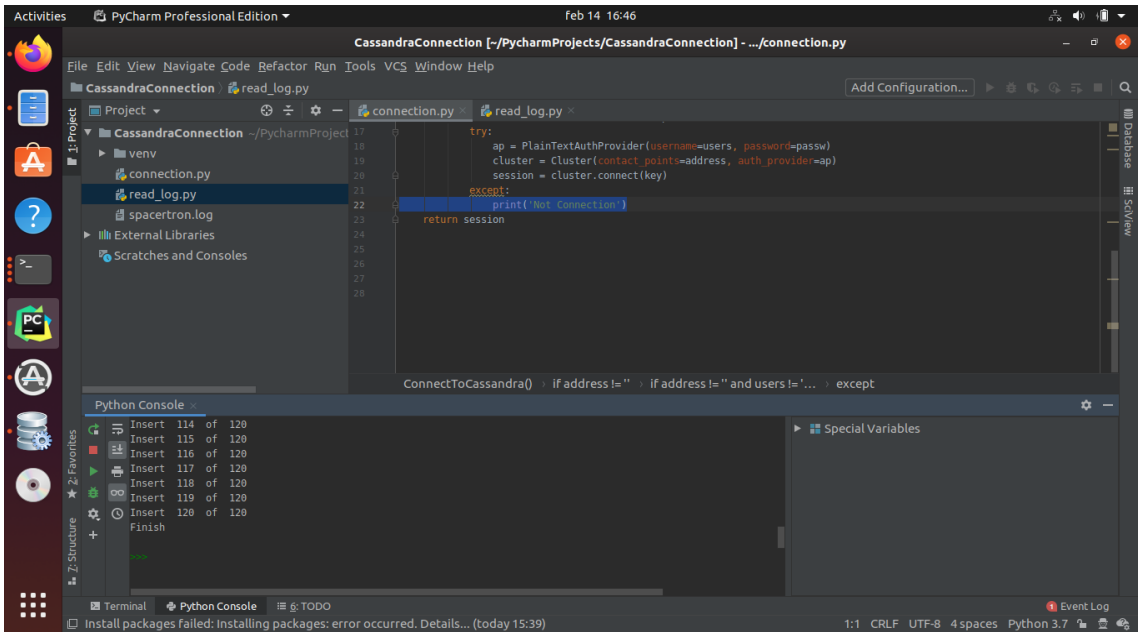

Figure 12. Cassandra read log operation.

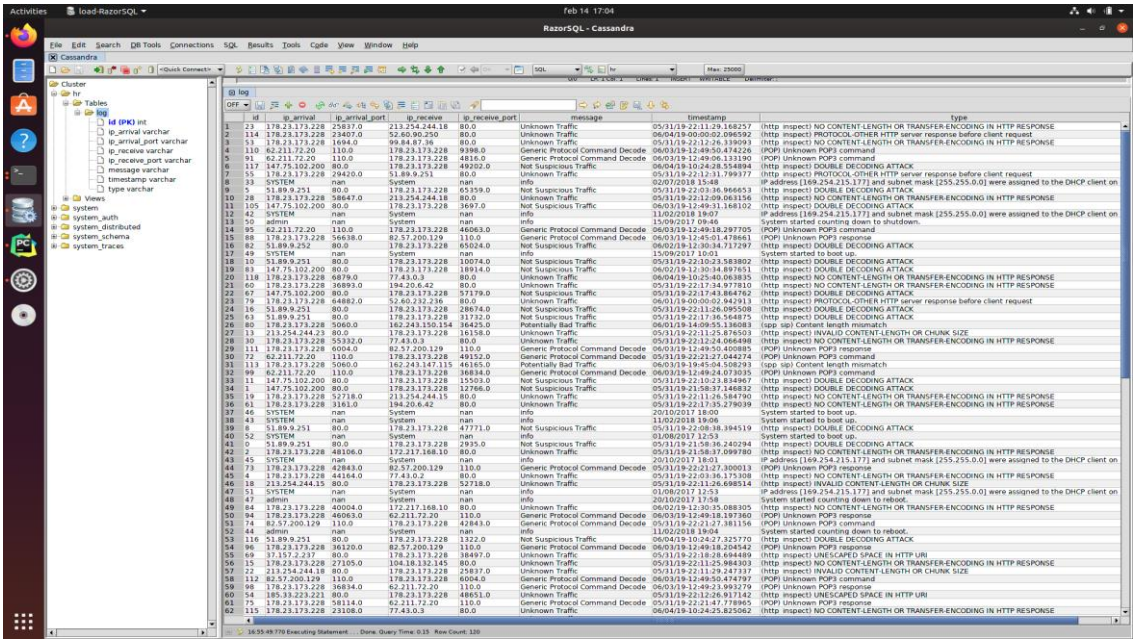

Figure 13. Created dataset in Cassandra NoSQL database.

5. CONCLUSION

The paper discusses the architecture of a platform managing multimedia data by optimizing server accesses and attacks detection by means of artificial intelligence algorithm and big data system. Specifically has been implemented a Tree Ensemble Learner algorithm predicting attacks by comparing log patterns, and using as a training dataset data stored into a Cassandra Big Data system. The results are achieved within the framework of a research industry project. This work could improve the experience using stream multimedia, in fields such as gaming, video calls, and VOIP calls.

6. APPENDIX: BIG DATA CONFIGURATION AND DATA STORAGE

In this section are reported the script of configuration of Cassandra Big Data system containing the training dataset of the Tree Ensamble model.

Cassandra linking:

connection.py

```
'''
Import libraries for connection to NOSQL Cassandra Node
'''
from cassandra.auth import PlainTextAuthProvider
from cassandra.cluster import Cluster
'''
Method used for connection to the node.
It returns the session.
'''
def ConnectToCassandra(address, users, passw, key):
    session = None
    if address != '':
        if address != '' and users != '' and passw != '':
            try:
                ap = PlainTextAuthProvider(username=users, password=passw)
                cluster = Cluster(contact_points=address, auth_provider=ap)
                session = cluster.connect(key)
            except:
                print('Not Connection')
    return session
```

Reading/writing scripts

read_log.py

```
import pandas as pd
from pprint import pprint as pp
from connection import ConnectToCassandra
# Method for open log file
def openlog():
    file =  pd.read_csv('spacertron.log',  delimiter="\t", header=None,
parse_dates=True,
                    names=['timestamp', 'type', 'message', 'ip_receive', 'ip_arrival',
'ip_receive_port',
                           'ip_arrival_port'])
    response = 'File opened.'
    print(response)
    write_log(file)
    return response
# Method for write the log on Cassandra's table called "log"
def write_log(log):
    '''
    Define parameters for the connections
    '''
```

```
keyspace = 'hr'
address = ['localhost']
users = 'linux'
passw = 'root'

for i in range(len(log)):
    ConnectToCassandra(address, users, passw, keyspace).execute(
        'INSERT INTO log (id, timestamp, type, message, ip_receive, ip_arrival, ip_receive_port,
ip_arrival_port) '
        'VALUES (%s,%s,%s,%s,%s,%s,%s,%s)',
        (i, log['timestamp'][i], log['type'][i],
         log['message'][i], log['ip_receive'][i],
         log['ip_arrival'][i], str(log['ip_receive_port'][i]),
         str(log['ip_arrival_port'][i]))
    )
    print('Insert ', i + 1, ' of ', len(log))
print('Finish')
```

ACKNOWLEDGEMENTS

The work has been developed in the framework of the research project: "Piattaforma ingegnerizzata per il management avanzato ad alte performance di dati multumediali con implementazione di nuove tecniche di cybersecurity 'ADVANCED MULTIMEDIA CYBER PLATFORM'" [High Performance Engineered platform for advanced management of multimedia data implementing new cybersecurity techniques: 'ADVANCED MULTIMEDIA CYBER PLATFORM'].

REFERENCES

[1] Massaro, A., & Galiano, A., (2020) "Image Processing and Post-Data Mining Processing for Security in Industrial Applications: Security in Industry," IGI Global 2020, Handbook of Research on Intelligent Data Processing and Information Security Systems, Ch. 6, pp117-146.

[2] Gañán, D., Caballé, S., Conesa, J., Barolli, L., Kulla, E., & Spaho, E., (2014) "A Systematic Review of Multimedia Resources to Support Teaching and Learning in Virtual Environments," *Proceeding of Eighth International Conference on Complex, Intelligent and Software Intensive Systems*.

[3] Li, F., & R. Lau, (2011), "Emerging Technologies and Applications on Interactive Entertainments," *J. Multimed*, Vol. 6, No. 2, pp 107-114.

[4] Ghanbari, M., (2011) "Standard Codecs: Image Compression to Advanced Video Coding," *Institution of Engineering and Technology*, ISBN-10: 0852967101.

[5] Arndt, T., & Katz, E., (2010) "Visual Software Tools for Multimedia Authoring," *Journal of Visual Languages & Computing*, Vol. 21, No. 3, pp184-191.

[6] Bovik, A. C., (2005) "Handbook of Image and Video Processing," Handbook of Image and Video Processing. A volume in Communications, Networking and Multimedia. Elsevier, 2nd Edition.

[7] Ani, U. P. D., He, H. M. & Tiwari, A., (2017) "Review of Cybersecurity Issues in Industrial Critical Infrastructure: Manufacturing in Perspective," *Journal of Cyber Security Technology*, Vol. 1, No. 1, pp32-74.

[8] Ali, B., & Awad, A. I., (2018) "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, Vol. 18, No. 3.

[9] Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M., (2016) "Smart Cities: A Survey on Security Concerns," *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 2, pp612-625.

[10] Lévy-Bencheton, C., & Darra, E., (2015) "Cyber Security for Smart Cities- An Architecture Model for Public Transport," ENISA report.

[11] Oliveira, L.M., Rodrigues, J. J., Sousa, A. F., & Lloret, J., (2013), "Denial of Service Mitigation Approach for IPv6- Enabled Smart Object Networks," *Concurrency and Computation: Practice and Experience*, Vol. 25, No. 1, pp129-42.

[12] Lo'ai, A. T. & Somani, T. F. (2016) "More Secure Internet of Things Using Robust Encryption Algorithms Against Side Channel Attacks," *Proceeding of IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*.

[13] Lo'ai, A. T., Somani, T. F., & Houssain, H., (2016) "Towards Secure Communications: Review of Side Channel Attacks and Countermeasures on ECC," *Proceeding of Internet Technology and Secured Transactions (ICITST) 11th International Conference*, pp87-91.

[14] Rohokale, V., & Prasad, R., (2015) "Cyber Security for Intelligent World With Internet of Things and Machine to Machine Communication," *Journal of Cyber Security*, Vol. 4, pp23-40.

[15] Tselentis, G., (2009), "Towards the Future Internet: a European Research Perspective," IOS Press, Netherlands.

[16] Badra, M., and I. Hajjeh, (2006) "Enabling VPN and secure remote access using TLS protocol," *Proceeding of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*.

[17] CTIA IoT White Paper, (2014) "Mobile Cybersecurity and the Internet of Things – Empowering M2M Communication," May 2014.

[18] Atzori, L., Iera, A., & Morabito, G., (2010) "The Internet of Things: A Survey," *Computer Networks*, Vol. 54, No. 15, pp2787-2805.

[19] Fleisch, E. (2010), "What Is The Internet of Things? – An Economic Perspective," Auto-ID Labs White Paper WP-BIZAPP-053

[20] Nagesh, S. (2013), "Roll of Data Mining in Cyber Security," *Journal of Exclusive Management Science*, Vol. 2, No. 5, 2013, pp2277–5684.

[21] Ansari, A. Q., Patki, T., Patki, A. B., & Kumar, V., (2007) "Integrating Fuzzy Logic and Data Mining: Impact on Cyber Security," *Proceeding of the Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*.

[22] Hongsong, C. (2011) "Security and Trust Research in M2M System," *Proceeding of IEEE International Conference on Vehicular Electronics and Safety (ICVES)*.

[23] Zeng, G., (2015) "Big Data and Information Security," *International Journal of Computational Engineering Research (IJCER)*, Vol. 5, No. 6, pp2250–3005.

[24] Moreno, J., Serrano, M. A. & Fernández-Medina, E., (2016) "Main Issues in Big Data Security," *Future Internet*, Vol. 8, No. 44.

[25] Massaro, A., Maritati, V., Savino, N., Galiano, A., Convertini, D., De Fonte, E., & Di Muro, M., (2018) "A Study of a Health Resources Management Platform Integrating Neural Networks and DSS Telemedicine for Homecare Assistance," *Information*, Vol. 9, No. 176, pp1-20.

[26] Massaro, A., Maritati, V., Giannone, D., Convertini, D., & Galiano, A., (2019) "LSTM DSS Automatism and Dataset Optimization for Diabetes Prediction," *Applied Sciences*, Vol. 9, pp3532.

[27] Massaro, A., Maritati, V., Savino, N., Galiano, A., (2018) "Neural Networks for Automated Smart Health Platforms oriented on Heart Predictive Diagnostic Big Data Systems," IEEE Proceeding AEIT 2018.

[28] Massaro, A., Maritati, V., Galiano, A., Birardi, V., Pellicani, L., (2018) "ESB Platform Integrating KNIME Data Mining Tool oriented on Industry 4.0 Based on Artificial Neural Network Predictive Maintenance," *International Journal of Artificial Intelligence and Applications (IJAIA)*, Vol. 9, No. 3, pp1-17.

[29] Massaro, A., Calicchio, A., Maritati, V., Galiano, A., Birardi, V., Pellicani, L., Gutierrez Millan, M., Dalla Tezza, B., Bianchi, M., Vertua, G., Puggioni, A., (2018) "A Case Study of Innovation of An Information Communication system and Upgrade of the Knowledge Base in Industry by ESB, Artificial Intelligence, and Big Data System Integration," *International Journal of Artificial Intelligence and Applications* (IJAIA), Vol. 9, No. 5, pp27-43.

[30] Massaro, A., Vitti, V., Galiano, A., & Morelli, A., (2019) "Business Intelligence Improved by Data Mining Algorithms and Big Data Systems: an Overview of Different Tools Applied in Industrial Research," *Computer Science and Information Technology*, Vol. 7, No.1, pp1-21, 2019.

[31] Massaro, A., Manfredonia, I, Galiano, A., Pellicani, L, & Birardi, V., (2019) "Sensing and Quality Monitoring Facilities Designed for Pasta Industry Including Traceability, Image Vision and Predictive Maintenance," *IEEE Proceeding of International Workshop on Metrology for Industry 4.0 and IoT*, pp68-72.

[32] Massaro, A., Manfredonia, I., Galiano, A., & Xhaysa,B., "Advanced Process Defect Monitoring Model and Prediction Improvement by Artificial Neural Network in Kitchen Manufacturing Industry: a Case of Study," *IEEE Proceeding of International Workshop on Metrology for Industry 4.0 and IoT*, pp64-67.

[33] D'Aloia, M., Russo, R., Cice, G., Montingelli, A., Frulli, G., Frulli, E., Mancini, F.,Rizzi, M., Longo, A. (2017) "Big data Performance and Comparison With Different DB Systems," *International Journal of Computer Science and Information Technologies*, Vol. 8, No. 1, pp59-63.

[34] Massaro, A. & Galiano, A. (2020), "Re-Engineering Process in a Food Factory: An Overview of Technologies and Approaches for the Design of Pasta Production Processes," Production & Manufacturing Research, Vol. 8, No. 1, pp80-100.

AUTHOR

Alessandro Massaro (corresponding author): Professor Alessandro Massaro (ING/INF/01, FIS/01, FIS/03) carried out scientific research at the Polytechnic University of Marche, at CNR, and Italian Institute of Technology (IIT) as Team Leader by activating laboratories for nanocomposite sensors for industrial robotics. He is in MIUR register as scientific expert in competitive Industrial Research and social development, and he is currently Chief of the Research and Development section, and scientific director, of MIUR Research Institute Dyrecta Lab Srl. Member of the International Scientific Committee of Measurers IMEKO, and IEEE Senior member, recently received an award from the National Council of Engineers as Best Engineer of Italy 2018 (Top Young Engineer 2018).