International Journal of Communication Networks and Information Security
2024, 16(S1)
ISSN: 2073-607X, 2076-0930
https://https://ijcnis.org/ **Research Article**

Comparative Sensory Data Monitoring Model Based On Multiple Algorithms between Server and Client PI within A Smart Manufacturing Setup

Tshepo Kukuni[1], Elisha Markus[2], Ben Kotze[3*], Adnan M. Abu-Mahfouz[4]

[1,2,3*,]Department of Electrical, Electronic and Computer Engineering, Central University of Technology, Free-State, South-Africa
[4]Council for Scientific and Industrial Research, Gauteng, Pretoria, South-Africa

Email: tgkukuni@gmail.com[1], emarkus@cut.ac.za[2], bkotze@cut.ac.za[3], aabumahfouz@csir.co.za[4]
Correspondence Email: [3*]bkotze@cut.ac.za

ARTICLE INFO

Received: 26 Apr 2024
Accepted: 02 Sep 2024

ABSTRACT

The optimal use of data in decision-making for instituting effective and efficient processes within the manufacturing sector is increasing rapidly. As a result, this digital transition poses high risk of cyber-attacks for various reasons such as financial gain etc. This research paper therefore aims at investigation the feasibility of a modelled system with the ability to correlate data between simulation model and physical model and the ability of such a model to cipher and decipher data without any losses. The presentation of such a model seeks to answer the research question looking at the impact of the encryption speed and its contributing to the data security quality and its influence in the implementation of security measures within a Smart Manufacturing Plant. The model setup was developed by creating two identical models based on the two PI4s and the application of the investigated algorithms on both PI4s with the same secret key that is used for both encryption (server-side) and decryption (client-side). Furthermore, the model setup was developed by implementing the shift rows and the mix column and inverse mix column on the 16X16 array based on the 128-bit-length. The results demonstrate that the developed model is secure and accurate without any loss of data. Furthermore, DES, Salsa29, RSA and DSA were tested and compared against each other utilising the same data file comprising of sensory data and the results demonstrate that all the five algorithms can cipher and decipher data without experiencing any data losses. However, the RSA and DSA execution times were 17ms and 21ms respectively, while the other AES executed at 4ns, DES at 3ns and Salsa29 2ns respectively. Therefore, this paper concludes that the investigated algorithms does provide high-level data-security, however, it is empirical to

further investigate the optimization of RSA and DSA algorithms to ensure efficiency.

Keywords: cyber-security, deep learning; internet of things; smart manufacturing plant; machine learning; intrusion detection; sensory data.

INTRODUCTION

The introduction of internet has become a key component in our daily lives and as such, businesses, schools, entertainment etc. relies heavily on it for aid. However, this reliance on internet-based services has predominantly led to a high rise in cyber-attacks. Cyber-attacks refer to any attempt to gain unauthorized access to a computer, computing system or network with the intent to cause damage [1]. In this instance, majority of authors predominantly refer to cyber-attacks as an external threat, however there are reported cases of internal cyber-attacks due to money, revenge, recognition etc. [2]. To enhance product quality, reduce cost, and improve business and manufacturing operations and ensuring sustainability, anomalies must be detected and eliminated or minimised early as to ensure data integrity [3]. Furthermore, to optimise and sustain the manufacturing plant, it is empirical to monitor and detect anomalies at an early stage by utilising models such as Intrusion Detection Systems (IDS) [4].

In developing such models, different kinds of data encryption algorithms are optimised and compared against each other based on the data encryption time and data losses based on encryption decryption results. As such the Data Encryption Standard (DES) despite being an old technology, it is also investigated against the other algorithms namely, 1) Advanced Encryption Standard (AES); 2) Rivest-Shamir-Adleman (RSA); 3) Digital Signature Algorithm (DSA); 4) Salsa29. DES encryption can be enhanced to either 2DES or 3DES by increasing the bit key length from 112-to-168-bit key length [5]. Data transfer between multiple devices are mainly data driven by the environment such as smart manufacturing environment that are prone to cyber-attacks. It is against this background that this research paper aims to investigate the encryption of data from the user to end-user and deciphering the encrypted file for human understanding and comparing the results against other know encryption algorithms based on the same data. This research paper aims at providing a scientific comparative output results to influence manufacturing plants managers in selecting the best data security algorithm for implementation that won't negatively affect the plant`s operations, efficiency, and productivity.

The remainder of this paper is as follows: Section 2 discusses the research questions, Section 3 presents the aims and objectives of this research paper, while Section 4 presents the related work both around the data encryption/ decryption as well as the advancements discovered to date. Section 5 presents the System technical development proposed with Section 6 presenting the results and discussion and the paper conclusion and contribution in Section 7.

Research questions

The use of cyber security encryption models for early detection of malicious cyber threats are predominantly increasing due to high elevation of wireless data transmission technologies that are currently in use within the smart manufacturing plants. However, despite the early detection and high-level data security, it is empirical to measure and compare the encryption/ decryption duration which would influence the decision for the enhancement of cyber-security in smart manufacturing plants. This research paper aims at investigating and responding to the following questions:

- Do currently available encryption algorithms have the capacity to transmit data over a non-secured network without losing or corrupting data?
- Does encryption speed duration play a role in data security quality?

3. Aims and objectives

This research paper aims at achieving the following objectives:

- To develop an encryption decryption model with the ability to compare textfile data against known algorithms for utilization in smart manufacturing plants;
- To model a decryption model with the ability to decipher point data from the encrypted file to measure any data losses during the process;
- To develop a sensory model that could correlate both simulation and practical input data and compare the cipher speed between different algorithms.

BACKGROUND AND RELATED WORK

The digital transition in manufacturing plants surfaces from conventional to digital where sensory data is critical for decision making such as early detection of systems malfunctions utilising other tools such as Augmented Reality (AR), mobile applications etc. as opposed to increasing number of SCADA systems. Ismaila et al. [6] presents a performance analysis on different classification algorithms by measuring algorithms performance based on variables such as accuracy, precision, Root Mean Square (RMS) of the symmetric algorithms hence the use of this algorithm in this research paper. The data comparison is essential in determining the best algorithm for utilization in smart manufacturing setup. Shende et al. [7] presents the efficacy for utilization of technological components such as machine learning. Shende presents the 16-bit binary numbers as an input to the developed sender neutral network. The results for the hamming distance were tested between the AES and RSA algorithms and the results outputs demonstrates that the AES is at 87.5% and RSA 98.25% respectively with machine learning approach at 65% hamming distance. Kenekayoro et al. [8] presents an overview of data encryption standards. This paper presents the criticisms around the security performance as well as the data confidentiality based on the encryption system. Figure 1 depicts the symmetric encryption model.

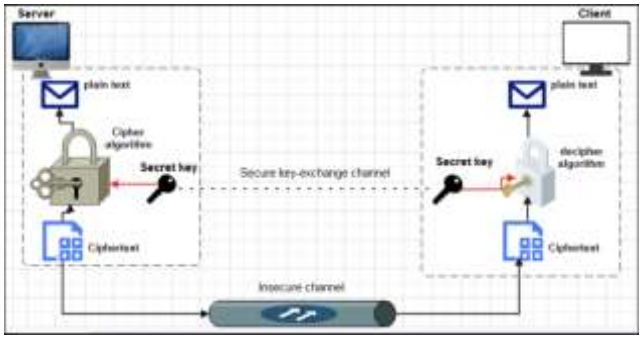


Figure 1. Symmetric cipher model.

Figure 1 depicts the encryption/ decryption symmetric model. The text is written as a simple plaintext input file and that is then sent to the "algorithm type". The client sends the plain text to the cipher algorithm (in this context each algorithm is used). After the file has been ciphered, the cipher text is then transmitted via Wi-Fi connection to the decipher algorithm utilising the same secret key and the file gets deciphered in the client side. Figure 1 presents the two equations; equations (1 and 2) based on the Figure 1 as follows:

$$C = E_k(P) \quad (1)$$

Where:
C = Cipher text; P = Plain text; K = key
Equation (1) occurs in the encryption side.

$$P = D_k(C) \quad (2)$$

Where:
P – Plaintext; D = Decipher text; K = Key
Equation (2) occurs in the decryption side.
Saad highlights that IoT is not exempted from cyber-attacks, in fact it poses high threats of cyber-attacks [9]. In retrospect, Badillo et al. [10] depicts that for AES system, only one secret key can be deployed for both encryption and decryption of plain texts by utilizing classification models such as AES-128/ 192 and/or 256, however, this research paper makes use of AES 128 bits. Furthermore, Kumar et al. [11] presents a model based on the modification of AES architecture to increase speed of producing subkeys. In the context of this research paper, the encryption time, data security and accurate data decipher were investigated. El-Attar et al. [12] presents the encryption strategy for converting static S-box algorithm to dynamic S-box algorithm. Furthermore, El-Attar makes use of RSA and Two fish algorithms to generate keys for the enhancement of privacy issues.
Nanjo et al. [13] presents efficient pairing calculation technique focusing on 128-bit security level. The results demonstrate the effectiveness and efficiency of the PC and Raspberry PI communication over the Barreto-Naehrig (BN) curve. Hawthorne et al. [14] compares the performance of Raspberry PI cluster to a power-efficient Next Unit of Computing (NUC) and a Mid-Range Desktop (MRD) on three leading cryptographic algorithms namely (AES, Twofish and Serpent) and assess the general-purpose performance of the three systems using the HPL benchmark. However, to standardize this research paper, all the algorithms were implemented on the same equipment, same data and two PI4s were used both on the client and server side.

5. System technical development

The proposed system model comprises of both hardware and software components. The parameters utilised in modeling the system hardware. Since the measured sensory data was not enormous (enormous in the context of this paper is data lower than 2MB) and the emphasis was on its security rather than properties such as low-cost sensors that were used in conducting this research.

5.1. Algorithm implementation

This research paper is based on the AES data encryption algorithm that is compared based on execution period against four cyber-security-based algorithms. AES algorithm is defined as a symmetric block cipher algorithm with a block size of 128 bits [15]. The algorithm implementation is based on Figure 2 AES model structure.

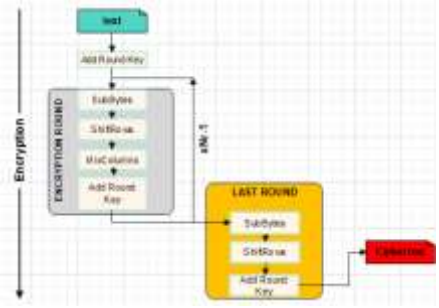


Figure 2. AES basic architectural model.

In this research paper, the encryption mode architecture was constructed based on 128 key bits as per the AES structure in Figure 2. Encryption models such as 1) shift rows; 2) Mix columns and 3) Add round key are used and implemented in the encryption of the sensory data. Shift rows – In this element, the second, third and fourth rows of the sensory data within the array matrix are shifted left in the order (1, 2 and 3) respectively. The first row of the matrix remains unchanged in this state. Mix columns – In this state, matrix multiplication is performed as follows by multiplying equation (1) and (2) functions as both mix columns and inverse mix columns.

$$\begin{bmatrix} A'1 \\ A'2 \\ A'3 \\ A'4 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01\ 01 \\ 01 & 02 & 01\ 01 \\ 01 & 01 & 03\ 03 \\ 03 & 01 & 01\ 02 \end{bmatrix} \begin{bmatrix} A1 \\ A2 \\ A3 \\ A4 \end{bmatrix} \quad (3)$$

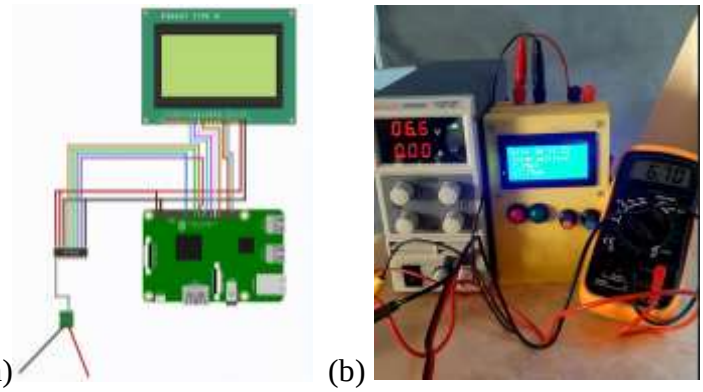
$$\begin{bmatrix} A'1 \\ A'2 \\ A'3 \\ A`4 \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d\ 09 \\ 09 & 0e & 0b\ 0d \\ 0d & 09 & 0e\ 0b \\ 0b & 0d & 09\ 0e \end{bmatrix} \begin{bmatrix} A1 \\ A2 \\ A3 \\ A4 \end{bmatrix} \quad (4)$$

Equations (3) and (4) depict the mix column element with A'1, A'2, A'3, and A'4 considered outputs after mix column and A1, A2, A3 and A4 considered input variables/ elements to the mix column process. Add round key - The performs function happens during the Add Round Key and as a result this operation can be reversible. The initial Add Round Key process generates subkeys during the key expansion process that are organized as a 4 x 4 state matrix. As part of the process, the inputs are transformed into new values as an output of each state into a value using the S-box array technique. In the context of this research paper, a 16x16 matrix was utilised that takes each input value where the first four values are used to define the table row as indicated in equation (3) and (4). Once this process is completed, the next four bits are set to define the new column i.e., for input byte CF, the output is 8A and the IS-box then reverses the process of the process of the S-box so that the DF refers to CF as indicated in the array model.

Sbox = [0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67,0x2b, 0xfe, 0xd7, 0xab, 0x76, 0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59,0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4,0x72]
#
ISbox = [0x52, 0x09, 0x6a, 0xd5, 0x30, 0x36, 0xa5, 0x38, 0xbf, 0x40, 0xa3,0x9e, 0x81, 0xf3, 0xd7, 0xfb , 0x7c, 0xe3, 0x39, 0x82, 0x9b, 0x2f,0xff, 0x87, 0x34, 0x8e, 0x43, 0x44, 0xc4, 0xde, 0xe9]

5.2. Hardware system development

Corel Draw and Proteus Simulation SoftwareTM were used for drawing of the enclosure and designing of the hardware physical model. Figures 3 (a-b) depicts the simulation model design and the physical model design, and both the simulation and physical model codes are executed.



(a) (b)

Figure 3a. Simulation model design; (b) Physical model design.

During the testing phase, current, voltage, time and date are retrieved and displayed on the LCD. However, this data`s focus is to be saved as a textfile since this data will be encrypted and shared between the PI server and decrypted in the PI Client. Once this process has been completed, a physical model is designed as indicated in Figure 3b to replicate the same results but with physical sensory data. Figure 3b depicts the hardware model, where the sensory data is compared against the multi-meter to ensure correctness and collaborative reading results. The power supply is used to vary the voltage that is then compared to the output in the multimeter and the LCD displays the data and this data is then saved as textfile before the encryption/ decryption can be applied.

5.3. System integration

The system development was based on both the software and hardware components. These models were developed and implemented with the purpose for having a complete uniform software and hardware system. Upon acquiring results based on individual tests, the integration was deemed necessary for the purpose of this research paper hence the simulation model in Figure 4.

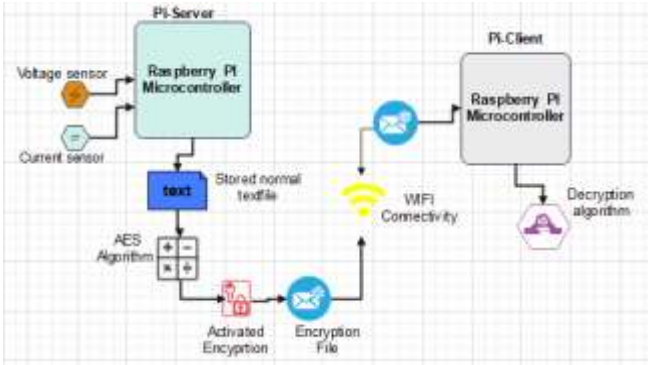


Figure 4. Simulation and integration model.

Figure 4 demonstrates the simulation model of the integrated software/ hardware model based on encrypted sensory data. The sensory data (voltage and current) is acquired through the PI Server, where the data is stored as a normal textfile. The AES algorithm is then applied to this textfile to cipher the data in the textfile. Once the file is successfully ciphered, the textfile is sent to the PI Client where the file is decrypted utilizing the reverse AES structure.

In testing the authenticity of the algorithm, the input encrypted file on the PI Server is as follows:

Input =
0.09,8.12,23/11/22,4:51\n0.09,7.94,23/11/22,4:51\n0.09,8.15,23/11/22,4:51\n0.09,5.90,23/11/22,4:51\n0.09,6.27,23/11/22,4:51\n0.09,6.52,23/11/22,4:51

After applying the AES algorithm, the result output is as follows:

Output =
p(y=\xe1\xbe\xc0\x80\xc1*AflH\xa24c\x88\xe6\x18z\x08\xe5*g\xd4\xc5\xa8\xe7\x11>4P\xb6\xf8\xddA}\xf7\xd74\x144b\xdd61\x0cr\x0f,\x12\x18Y\xa5\xbe\t\xea\xaf\xc9\x7fL\x83\xfbQ\xa7\xd5\x1e\xe4\x00\xa0\x97>K\x83\xe1cd\x1f)

In the client side the input becomes the output from the serve which is the encrypted data file.

Input =
p(y=\xe1\xbe\xc0\x80\xc1*AflH\xa24c\x88\xe6\x18z\x08\xe5*g\xd4\xc5\xa8\xe7\x11>4P\xb6\xf8\xddA}\xf7\xd74\x144b\xdd61\x0cr\x0f,\x12\x18Y\xa5\xbe\t\xea\xaf\xc9\x7fL\x83\xfbQ\xa7\xd5\x1e\xe4\x00\xa0\x97>K\x83\xe1cd\x1f)

Output =
0.09,8.12,23/11/22,4:51\n0.09,7.94,23/11/22,4:51\n0.09,8.15,23/11/22,4:51\n0.09,5.90,23/11/22,4:51\n0.09,6.27,23/11/22,4:51\n0.09,6.52,23/11/22,4:51

RESULTS AND DISCUSSIONS

The results obtained from the model test has demonstrated the ability of the AES algorithm to cipher and decipher a plain textfile with sensory data and allowing the model to transfer the same textfile between two devices using over the Wi-Fi connection. The system development testing proved to be very effective and reliable with both sensory data output on the system correlating with multi-meter (physical) output results. However, this was not the primary focus of the research, but rather to use AES algorithm on the sensory textfile and evaluating its accuracy in both transferring data without any losses and the time it takes to executive the algorithm. Furthermore, the research investigated the decryption of the accuracy of the data and the comparison between AES algorithm against the already labelled algorithms.

(a) (b)

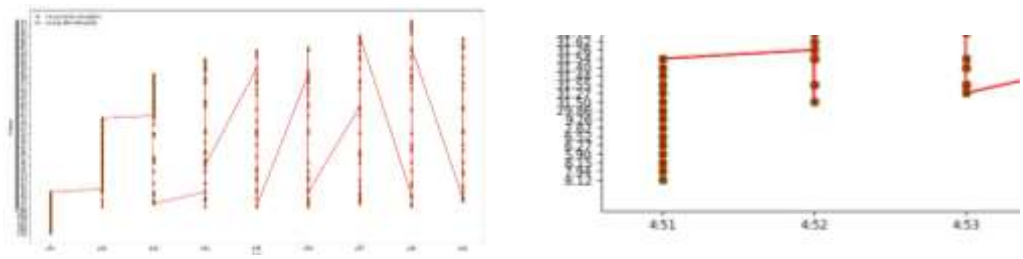
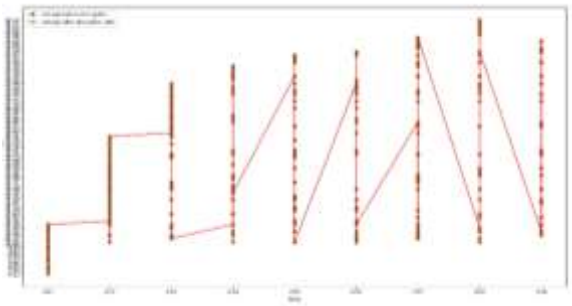


Figure 5a. Data accuracy encrypted input data and decrypted output data (time vs voltage); (b) Zoomed version Figure 5a.

Figure 5a presents the data accuracy for both encryption and decryption algorithms and furthers outlines the points in which the voltage value is encrypted and decrypted. The results demonstrate that every reading was able to be encrypted and decrypted per minute without experiencing any losses.

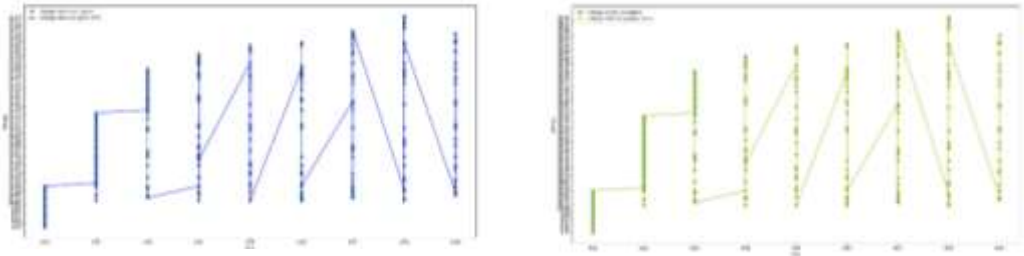
Figures 6 (a – e) depicts the results output model based on the four commonly known algorithms that are benchmarked against the AES algorithm results.



(a)

Figure 6a. AES modelled results.

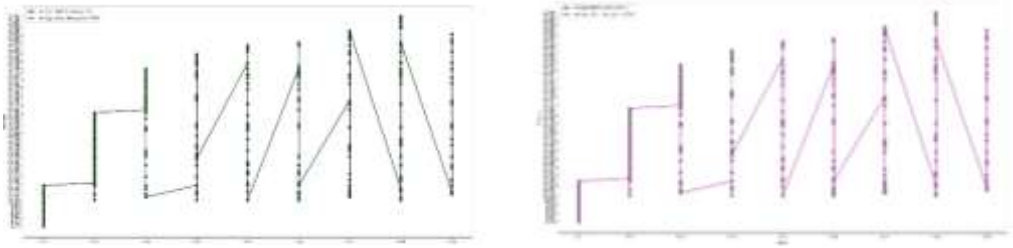
The results presented demonstrates the ability of AES based algorithm in successful execution of data encryption and decryption per data point without any data losses within a smart manufacturing environment through Wi-Fi connection. Figure 6a presents a positive data accuracy output results at period of 4ns that it takes to execute the encryption algorithm.



(b) (c)

Figure 6 b). DES modelled results: c) Salsa modelled output results.

Figures 6 (b-c) presents the DES and Salsa29 model results respectively. The results show that in both tests conducted, encryption and decryption occur at each point which demonstrates that the model can successfully retain data from the encryption point to the decryption point. However, both algorithm`s encryption time is 3ns and 2ns respectively which demonstrates that their execution period difference is not significant and in such a case, the selection of the model will be the prerogative of the manufacturing plant manager.



(d) (e)

Figure 6 d). RSA modelled results; e). DSA modelled results.

Figures 6 (d-e) presents the RSA and DSA model results respectively. The results show that in both tests the encryption and decryption occurs at each point which demonstrates that the model can successfully retain data from the encryption point to the decryption point. However, both algorithm`s encryption time is 17ms and 21ms respectively.

In comparing the encryption reliability of the model, the model`s output benchmarking was conducted based on the time it takes the algorithm to execute the encryption process and the reliability of the encrypted data transfer between the client and server. The reason for the utilization of time as factor was due to successful encrypt and decrypt of the plain textfiles,

however, the major difference was the time it took mainly around the encryption duration of the file. Figure 7 depicts the graphical overview of the encryption execution time.

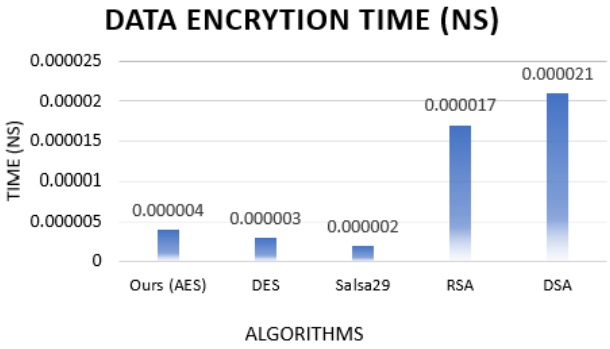


Figure 7. Graphical results overview based on encryption execution time.

Figure 7 presents the graphical overview in nanoseconds for the encryption execution time. Based on the five investigated algorithms, the "ours-AES, DES and Salsa29 which were able to executive the encryption at 4ns; 3ns and 2ns respectively as compared to the RSA algorithm that took 17ms to execute while DSA spun-out at 21ms seconds. The research paper findings have therefore demonstrates that both symmetric and asymmetric encryption decryption algorithms are capable of successfully transmitting data via Wi-Fi connection without any data losses. However, it is crucial to optimise the RSA and DSA to obtain swift encryption execution time.

7. Conclusion and contribution

The development of secure data encryption is critical in the manufacturing of plants, hence the need for continuous investigation for methods to counter hacking and cyber threats. This research paper therefore concludes that it has achieved the research aims and objectives and has demonstrated the feasibility for the development and implementation of a data encryption/decryption model that performs without experiencing any data loss and data discrepancy within the smart manufacturing setup.

Furthermore, it was noted that RSA and DSA algorithms had longer delay duration in the execution of the encryption process as opposed to other algorithms, notwithstanding the fact that the data security and reliability remains intact which demonstrates the effectiveness of these investigate algorithms in data security. Due to increase in machinery within the smart manufacturing plants, reliance on accuracy and speed is not enough to measure the model performance mainly with small data files hence the need to investigate such model in the future will require system resilience tests not only focusing on cyber-security but also processing time that would influence the purchasing of new equipment etc.

This paper has contributed to the modeling and implementation of a sensory data modelling system that can be used to investigate the accuracy of data in two separate models. Furthermore, this research paper has contributed to the optimisation and use of dynamic data to influence the decision making within for the best secure and efficient algorithm based on time it takes to cipher data. The results of this paper will assist plant managers to coerce informed decisions.

Acknowledgements

We acknowledge the efforts of Mr Lepekola Lenkoe for the assistance in code optimization.

REFERENCES

[1] M. Pratt, "Techtarget Security," Techtarget , August 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/cyber-attack. [Accessed 23 May 2023].

[2] J. Pande, "Introduction to cyber security," Uttarakhand Open University, 2017, pp. 16-19.

[3] M. Gamal, A. Donkol, A. Shaban, F. Constantino, G. Di Gravio and R. Patriarca, "Anomalies detection in Smart Manufacturing using machine learning and deep learning algorithms," pp. 1611-1622, 2-5 August 2021.

[4] T. Kukuni, E. Markus, B. Kotze and A. Abu-Mahfouz, "Development of IoT-Based Machine Learning Application for Data Anomaly Detection Within a Smart Manufacturing Plant," vol. 20, no. 10, pp. 3637-3648, August 2022.

[5] B. Vyas and A. Vajpayee, "Local Data Security Thought Encryption," IJSART, vol. 2, no. 8, pp. 10-15, August 2016.

[6] S. Abdulhamid, M. Shuaib, O. Osho, I. Ismaila and J. Alhassan, "Comparative Analysis of Classification Algorithm for Email Spam Detection," IJ Computer Network and Information Security, vol. 1, pp. 60-67, 2018.

[7] V. Shende and M. Kulkarni, "Application of Machine Learning in Cryptography," Advnaced trends in computer science and engineering, vol. 9, no. 3, pp. 3460-3462, 2020.

[8] P. Kenekayoro, "The data encryption standard thrity four years later," African Journal of Mathematics and Computer Science Research, vol. 3, no. 10, pp. 267-269, 27 August 2010.

[9] M. Saad and R. Soomro, "Cyber security and internet of things," Pakistan Journal of Engineering Technology and Science (PJETS), vol. 7, no. 1, p. 77, 2017.

[10] A. Badillo, R. Gutierrez, M. Rosales, P. Bautista and F. Uribe, "Hybrid Pipeline Hardware Architecture Based on Error Detection and Correction for AES," Sensors, vol. 21, no. 16, p. 5655, 2021.

[11] T. Kumar, K. Balmuri, A. Marchewka, P. Divakarachari and S. Konda, "Implementation of speed-efficient key-scheduling process of AES or secure storage and transmission of data," Sensors, vol. 21, no. 8347, pp. 1-17, 2021.

[12] N. El-Attar, D. El-Morshedy and W. Awad, "A new hybrid automated security framework to cloud storage system," Cryptography (MDPI), vol. 5, no. 37, pp. 1-20, 2021.

[13] Y. Nanjo, M. Khandaker, T. Kusaka and Y. Nogami, "Efficient pairing-based cryptography on Raspberry PI," Journal of Communications, vol. 13, no. 20, pp. 88-93, February 2018.

[14] D. Hawthorne, M. Kapralos, R. Blaine and S. Matthews, "Evaluating cryptographic performance of Rasperry PI Cluster," pp. 1-9, 22-24 September 2020.

[15] B. Jena, "Simple Learn," 11 2022. [Online]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption. [Accessed 14 11 2022].

Authors

Dr Tshepo Kukuni: Senior Manager: Fleet and ICT (Matjhabeng Local Municipality)
tgkukuni@gmail.com: - 0714571911

Tshepo Godfrey Kukuni holds a Doctoral degree in Electrical Engineering, and he has worked both in industry and academia and he's also a Director at Rea Thusa Consulting Engineers (PTY) LTD. Dr Kukuni has published papers in different journals both nationally and internationally. Dr Kukuni is also currently working on research on Network Intrusion Detection applications, Augmented Reality Applications, Free-Piston Engines, Image Processing, Computer vision, Machine Learning, Design and Modelling, and Machine Vision. Dr Kukuni is also a registered member of the South African Association of PhDs (SAAPhDs) and his also on the Advisory committee on Innovation at Institute for the Study of Legislature in South Africa (ISLSA) and Technology Innovation Station (Tshwane University of Technology - TUT).

Prof. Elisha Markus: Senior Lecturer at CUT, FS
emarkus@cut.ac.za: - 0744062563

Prof Markus holds a Doctoral degree in Electrical Engineering. His research interests are in Robotic control, smart networks, WSNs, IoTs, machine learning, assistive mobility technologies and electromagnetic fields. He is currently working on cooperative robotic systems in health care and mining applications at the Center for sustainable smart cities at the Faculty of Engineering, Built Environment and Information Technology (FEBIT). He is employed in the Faculty of Engineering, Built Environment and Information Technology at the Central University of Technology, Free State. He is also actively involved in the Centre for Sustainable Smart Cities.

Prof. Ben Kotze: Assistant Dean at CUT, FS
bkotze@cut.ac.za: - 08285318755

Ben Kotze holds a Masters and Doctoral degrees in Electrical Engineering. He is professionally registered with the Engineering Council of South Africa (ECSA) and several associations of which the oldest South African Institute of Electrical Engineers (SAIEE est. 1904) where he is a fellow. With seven years, industry experience and over thirty years tertiary education experience in Electrical Engineering of which he lectured more than 23 subjects. He is still actively involved with industry and work integrated learning (WIL). He is currently doing research on vision, several different AGV's, renewable energy systems, simulation and control, augmented reality systems, IoT security, smart farming,

and prediction methods. Several undergraduate students, masters and doctoral passed by his mentorship.

Prof. Adnan M. Abu-Mahfouz

Adnan M. Abu-Mahfouz ((Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2005 and 2011, respectively. He is currently a Chief Researcher and the Centre Manager of the Emerging Digital Technologies for 4IR (EDT4IR) Research Centre, Council for Scientific and Industrial Research; an Extraordinary Professor with University of Pretoria; and a Professor Extraordinaire with the Tshwane University of Technology, Pretoria; South Africa. His research interests are wireless sensor and actuator network, low power wide area networks, software-defined wireless sensor network, cognitive radio, network security, network management, and sensor/actuator node development. Prof Abu-Mahfouz is a Section Editor-in-Chief with the Journal of Sensor and Actuator Networks, an Associate Editor at IEEE INTERNET OF THINGS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON CYBERNETICS, and IEEE ACCESS, and a member of many IEEE technical communities.