International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V71I3P201

Volume 71 Issue 3, 1-8, March 2023
© 2023 Seventh Sense Research Group®

Original Article

Secure and Optimized Communication in the Internet of Things using DNA Cryptography with X.509 Digital Attributes

S. Karthikeyan[1], T. Poongodi[2]

[1,2]*School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India*

[1]*Corresponding Author : link2karthikcse@gmail.com*

Received: 26 October 2022 Revised: 10 February 2023 Accepted: 25 February 2023 Published: 25 March 2023

Abstract *- The Internet of Things (IoT) is a large volume of physical entities that forms large interconnections between them and then connect with the internet to establish communication for improving the quality of human life. The exchange of data between these entities can lead to attacks or modifications of sensitive data. Hence, data authentication is regarded as a vital requirement to access the system for secured message transmission. The security of data is achieved by proper data authentication. Hence, in this paper, the major objective of the proposed system is to deliver secure and optimized communication in the Internet of Things using DNA cryptography with X.509 certificates, here by using X.509 digital certificates to produce attributes for key generation based on the data and DNA cryptography to secure the data, which hides the genetic information using a computational method to improve data privacy in DNA sequencing processes. Here the result gives DNA-X.509 gets a reduced key size after encoding using DNA-X.509 than the one with DNA and ECDSA algorithms. The application of attributed-based X.509 also improves the authentication ability of the data compared to the other methods. X.509 digital certificates and DNA cryptography to secure the data that hides the genetic information using a computational method for improving the data privacy in DNA sequencing processes*

Keywords *- IoT, DNA Cryptography, Authentication, Privacy, X.509 Certificates, Cryptosystem, Authorization.*

1. Introduction

With Cloud and informatics applications at the heart of everyday life, the Internet of things (IoT) is a new class of services that increases our dependency on networked technologies even more than we might have imagined only a decade ago [1]. Although IoT devices and services explicitly aim to provide significant benefits, the security threats posed by Internet access should be apparent [2]. It is generally recognized that numerous threats occur on the Internet, and extends the scope of those threats to ordinary devices [3]. In addition, above and beyond vulnerability to bad actors' harmful activities, there are additional issues for those who may rely on IoT goods and services that the possibility is inoperative over deprived connectivity with the internet that arises either from the breakdown of network segments or technical difficulties. In 2017 alone, attacks on IoT devices grew by 600% [4,38]. Their involvement in breaching IoT systems increased, as well as increased measures for IoT system security were emphasized [5] [6] [7].

Security breaches have been commonly publicized for longer than the Internet is commercially available [8]. It was non-malicious evidence of the idea, which over a decade afterwards, may have brought down the Internet. Since then, there have been numerous internet threats [9]. Unfortunately, these threats appear to pose a rising danger to the security and fidelity of internet networks as we become increasingly reliant on the Internet in our everyday lives [10,11]. Trade and key networks are not only the object of trade but also increasingly ordinary products such as alarms, appliances, video cameras, door locks, and various devices connected to the Internet [12]. Although early Internet security issues may have been troublesome, they were, in a way, disconnected from the network. Today, the actual presence of these threats is much stronger than in the past [13].

Present IoT gadgets also outnumber internet communications, including cell phones and computers [7]. It should be noted. This trend is predicted to lead to over two trillion dollars in IoT market value by 2023. However, this still offers those who are unable to take advantage of this booming market a much bigger chance [14]. The explanations for these intrinsic flaws vary from the insouciance of providers who hurry to sell goods to advanced malware schemes to thwart conventional security procedures [15]. The criminal tendency to command network-linked computers has enabled ever more powerful forms of brutes, and a new breed of botnet forces, with a variety of ways to create untold riches, has been created by the criminal tendency to command network-linked computers [16]. Security risks are normally a secondary issue at the same time. These factors are a major challenge for the security forces which secure the information technology on which we depend [17-19]. In this paper, X.509 digital certificates [20,21] are used to produce attributes for key generation based on data [44] and DNA cryptography [22-26] to secure the data, which hides the genetic information using a computational method for improving the data privacy in DNA sequencing processes.

In this paper, research is still being carried out for IoT Security and the right authentication mechanism to prevent hackers. Related work describes the authors' research work relevant to DNA cryptography and security. In the Proposed mechanism, implementation of DNA cryptography with X.509 Digital Certificates in the IoT with results carried out and the conclusion.

The Contribution of research work is summarized as follows

1. Designing DNA Cryptography and combining the x.509 digital certificate helps to detect intruders in an IoT environment.
2. The proposed DNA and digital certificate, compared with ECDS encryption, outperformed the existing methodology.

The remaining paper is structured as a literature survey in section 2, then proposed work in section 3, results and discussion in section 4, and then the conclusion in section 5.

2. Literature Survey

IoT brings the Internet's edge into our daily lives by allowing modern computers that were previously available offline to connect to the Internet. Because of the rapidity with which these products are being introduced, research and true safety design will become an incentive for innovative products to enter the market ahead of the competition since it is not enough, unlike the previous IoTs, where it does not normally operate with the relative safety boundaries of data cisers but are easily reachable by someone who might attempt to manipulate any bugs within the IoT system by physical access [27]. Moreover, because IoT devices frequently lie inside the walls of our houses, workplaces, and places open to the public, they can be used to spy on suspicious people in the near physical vicinity of their equipment if these devices are affected [28].

The vulnerabilities of IoT systems differ considerably according to the 7-layer reference model. Physical computers are clearly susceptible to several potential attack modes because of their physical availability. To obtain access to the whole machine, an attacker or the intruder can provide physical access, manipulation, and potentially a reverse engineer. The communications layer is also a visible surface of attack since the Internet is used as the medium of communication and is considered vulnerable to multiple forms of protocol attacks, from famous attacks to unknown attacks. However, these levels frequently have applications bugging in third-party code and systems that could be disrupted or infiltrated by edge computing, data accumulation, and network abstraction. Poorly written SQL injecting applications and other forms of attacks used to hack data stores will also be the target.

Xiao et al. [46] and others discussed numerous problems that designers of IoT systems are experiencing, especially the shortcomings associated with the computation of edge devices.

Meidan et al. [30] suggested a training model using the random forest to predict unauthorized devices on this network. Doshi et al. [31] tested multiple predictive model models trained with several popular algorithms of learning machines. They found a high-efficiency level utilizing what they call stateless features, identified as flow-independent features of each packet. Compared to stateful features, these were found to perform well as features that capture changes in traffic on the network over time. Even the Internet of Things is considered an intelligent segment, and researchers were carrying out work on machine learning algorithms for security issues [30-32,46].

Research has shown that machine learning technology is useful in addressing security issues in the network. Moskovitch et al. [33,34] swed more than 90% accuracy in forecasting worm activity and used machine learning to detect malicious behaviors in a computer. Different ways of dealing with these attacks have been suggested since Stuxnet. For many models over 90%, Ponomarev and Atkinson [47] discussed master-learning approaches with accuracy. The advanced multi-level security attacks call for machine learning methods, Nath and Mehtrel [36] concluded.

DNA cryptography combined with soft computing has been suggested for increased security measures in the cloud, and various cryptography approaches with performance and limitations are described [42].

Fog computing is suggested as a way of maintaining massive data of IoT and improving safety [19]. However, this approach introduces new vulnerabilities which reduce potential safety gains. Fog computing reduces traffic from and to IoT core processing considerably, but it adds uncertainty that enhances difficult authentication, secures transitional data, and safeguards the privacy of users [37]. Using DNA cryptography with steganography, data will be encrypted using a secret Key and then concealed in the image, which helps prevent attacks from intruders [41].

Machine Learning (ML) models will help prevent, detect, and disrupt cyberattacks in the initial stage. Feature Selection Strategies (FSS) improve ML model performances applied to cybersecurity for DOS-DDOS attacks [38].

Here an IoT design made up alarms system implemented in suspicious locations. The alarm alerts the user via the mobile application, which can reduce robbery [39].

The various IoT data collected through sensors should be stored on the cloud with security, various encryption methods, and data privacy schemes, threats and privacy challenges are discussed [40].

3. Proposed Method

Cryptography is integral to the system security model and protects the attacks on sensitive data and documents. Generally, every existing cryptosystem has these components and algorithms [1]:

- Plaintext
- Cipher text
- Key
- Encryption Algorithm
- Decryption Algorithm
- Key Generation Algorithm

Figure 1 illustrates the components used in the cryptosystem.

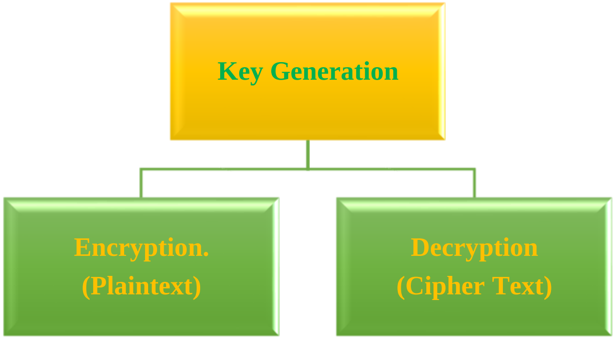

Fig. 1 Cryptosystem Components

3.1. DNA Cryptography

DNA is a compound that contains genetic material and stands for deoxyribonucleic acid in living organisms. It also carries inherited material in the form of chromosomes. Nucleotide is the core component of DNA molecules. The following are the different nitrogen bases:

- Adenine (A),
- Cytosine (C),
- Thymine (T), and
- Guanine (G).

Different combinations of these bases will store information. Ribo Nucleic Acid (RNA) is based on DNA, where Thymine (T) will be replaced by Uracil (U).

DNA can store information more than binary strings since they are expressed by alphabets {A, C, T, G} compared to binary strings represented in terms of an alphabet {0,1}. Binary strings 00, 01, 10, and 11 are used in the present work for the designation of A, C, G, and T. DNA molecules in a compact form can store information in addition to massive data storage.

The cryptography components used in the cryptographic scheme are [43]:

- DNA sequencing: baseline sequences are calculated in DNA.
- DNA encoding: a mechanism where a certain plaintext can be translated into a series of DNA bases.

(00 → A, 01 → C, 10 → G and 11 → T).

Molecular biology has provided insight into transcription and translation biological processes, which are debated as follows:

- Transcription and Translation

3.1.1. Encryption

Here the encryption algorithm comprises [43].

- Genetic Code Conversion: Genetic Code conversion occurs when a binary element is converted to DNA.
- Transcription: This is the mechanism by which DNA type has been converted to mRNA.
- Translation: This is the method to translate the mRNA type into a protein base cipher document.

The encryption algorithm consists of translating the sender's legible text into the receiver's chip text. Using Huffman encoding, the readable text is translated into binary. This will make XOR easier in any round with the sixteen-bit size. The binary form will be XORed, which is later encoded into a DNA genetic code. The translation is conducted to translate DNA into mRNA. The translation follows to transform the mRNA into a protein type that gives the text.

3.1.2. Key Generation - X.509 Attribute Certificate

A bidirectional associated neural memory network (BAMNN) is trained to produce keys for each respective data cube. Random generation of the first block and the generation of more blocks using the BAMNN mechanism. Figure 2 illustrates the architecture of the encryption method and its key generation algorithms. A neural network with associative memory is mainly used for the key generation process. The weight matrix W is used for the neural network weights. It is a matrix of 16x16x256 weights in this case.

A more effective means of authenticating a customer and monitoring his or her privileges is to inspect the Authority Certificate (AC) in a repository instead of approving the client's ACs. This approach will summarize the security benefits following:

- A requesting party should query a trustworthy database without relying on actual or modified customer information.
- Access to the registry will be protected and efficiency improved if the normal way is correct to examine the credentials of these attributes.
- Simplifies the authorization process, so the recipient does not have to explain the rights directly to the applicant body (Fig. 3).

As this approach becomes the primary method of questioning a user's rights, the libraries that contain these credentials should be considered in scale and have top-quality access to them. However, the information on deployment includes the selection of special technology on distributed networks and is not subject to the document.

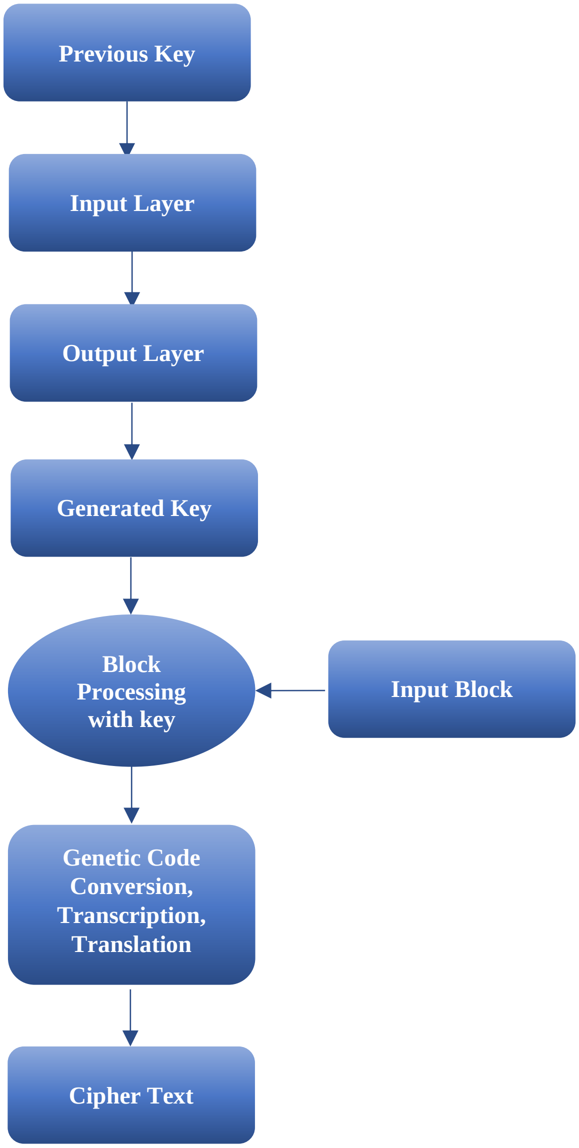
Previous Key
Input Layer
Output Layer
Generated Key
Block Processing with key
Input Block
Genetic Code Conversion, Transcription, Translation
Cipher Text

Fig. 2 Key Generation

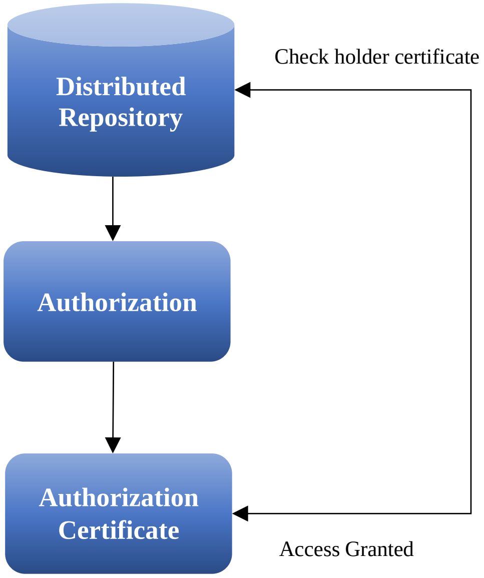

Fig. 3 x.509 Attribute Certificates

3.1.3. Decryption Algorithm

The decryption algorithm consists of,

- Reverse Translation: This is the mechanism by which the protein base cipher text is converted into mRNA shape.
- Reverse Transcription: Transform mRNA to a DNA type through this procedure.
- Genetic Code - Reverse Conversion: Translating the DNA into binary form into a genetic code.

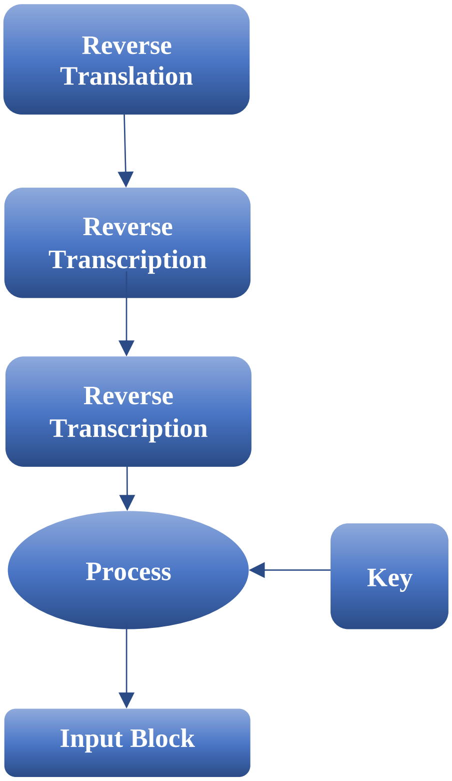

Fig. 4 Decryption Algorithm

Python simulates the above decryption processes. In the case of reverse translation, a major difficulty was in which one or several maps had a protein basis and 3 mRNA. This dilemma has been resolved by hacking. The transfer of the protein base to the shape of mRNA was thus possible. The padded 'N' or 'NN' string was deleted during this procedure at the end of the resulting mRNA. The reverse transcription mechanism was simulated by translating the uracil basis into thymine. The translation from mRNA to DNA was made possible.

When the DNA form was converted to binary, the reverse translation was simulated using the genetic code during the mapping of DNA into binary form. Then the XORed Binary form is considered a key to this particular round, and k is used to delete the padded zeroes. Further, the Huffman decoder does plain text decryption of the original form. The decryption algorithm architecture is shown in the proposed cryptosystem in Figure 4.

4. Results and Discussions

In this section, the modified DNA algorithm is simulated in Python with a 2.4GHz computing engine and 16 GB RAM. The model's performance is tested under different performance metrics that include: encoded key size, signature time, and key generation time in terms of its minimum, average, and maximum time. The proposed method is compared against the DNA model and ECDSA [34].

Here x-axis denotes the encoded key size, whereas the y-axis represents the key size, as can be seen for the 128 key sizes of DNA-X.509 obtained a reduced key size than the ECSDSA DNA. Then Figure 5 shows the results of the encoded key size vs the original key size, where the result shows the DNA-X.509 obtains reduced key size after encoding using DNA-X.509 than the one with DNA and ECDSA algorithms. The utilization of attributed-based X.509 further improves the authentication ability of the data than other methods.

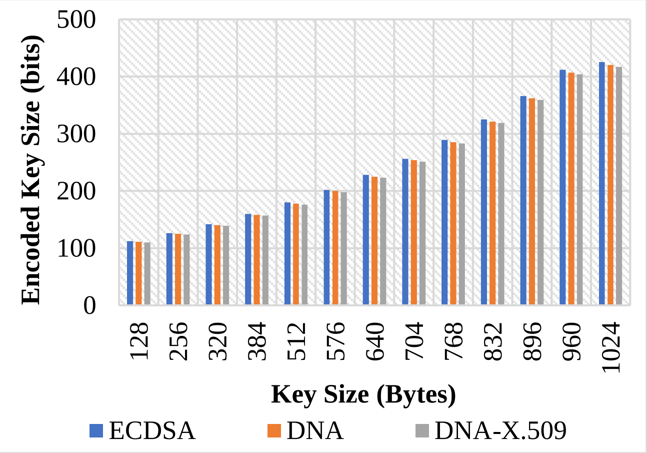

Fig. 5 Encoded Key size vs original key size

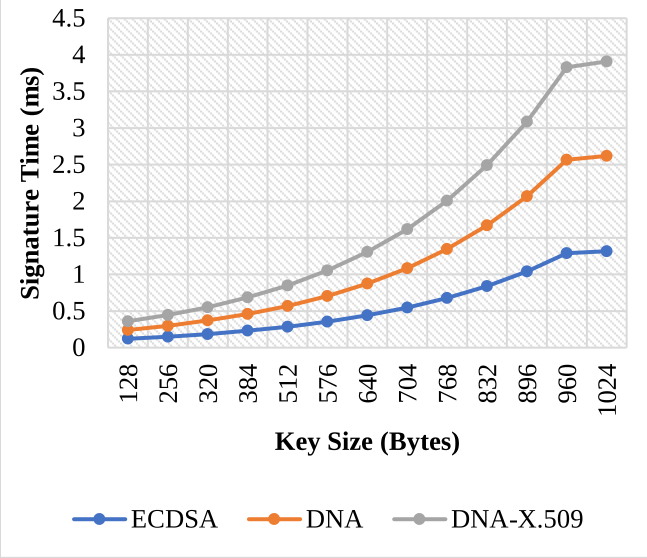

Fig. 6 Signature Time (ms) vs Key size (Bytes)

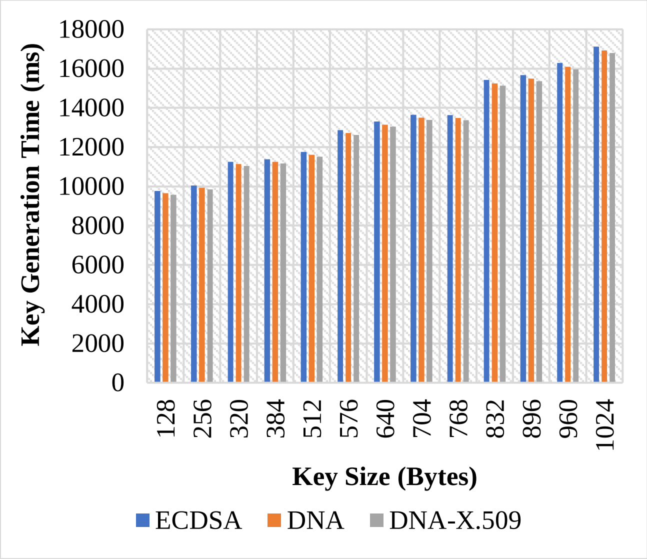

Fig. 7 Key Generation Time (ms) vs Key size (Bytes)

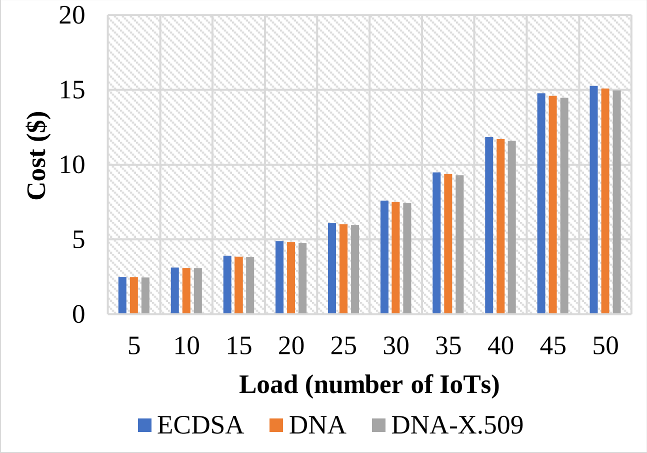

Fig. 8 Load vs Cost

Here x-axis represents signature time, and the y-axis represents key size with the comparison of ECDSA, DNA, and DNA-X.509. Initially, the signature time for ECDDSA in 128 key sizes is 0.2, then for DNA, it is near 0.3 and then for DNA-X.509, it is 0.4. Thus Figure 6 shows the results of Signature Time (ms) vs Key size (Bytes), where the result shows that the DNA-X.509 obtains reduced signature time after encoding using DNA-X.509 than the one with DNA and ECDSA algorithms.

In figure 7, the x-axis denotes key generation time, and the y-axis represents the key size, where DNA-X-509 for 128 key size takes 9568 key generation time, and the result shows that the DNA-X.509 obtains reduced key generation after encoding using DNA-X.509 than the one with DNA and ECDSA algorithms.

Here in figure 8 x-axis represents the load, and the y-axis represents the cost. The cost for ECDSA, DNA, and DNA-X.509 are 15.26,15.09,14.96, which signifies the cost reduction when using DNA-X.509 in an IoT environment.

5. Conclusion

In this paper, X.509 digital certificates are used to produce attributes for key generation based on the data and DNA cryptography to secure the data, which hides the genetic information using a computational method for improving data privacy in DNA sequencing processes. The simulation results show that the proposed method achieves more reduced encoded key size, signature time, and key generation time than the existing DNA model and ECDSA algorithm.

References

[1] Sanaz Nakhodchi, Aaruni Upadhyay, and Ali Dehghantanha, “A Comparison between Different Machine Learning Models for IoT Malware Detection,” *Security of Cyber-Physical Systems, Springer, Cham*, pp. 195-202, 2020. [CrossRef] [Google Scholar] [Publisher link]

[2] Tejasvi Alladi et al., “Consumer IoT: Security Vulnerability Case Studies and Solutions,” *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17-25, 2020. [CrossRef] [Google Scholar] [Publisher link]

[3] Henry K. H. Wang, *Renewable Energy Management in Emerging Economies: Strategies for Growth*, Routledge, 2020. [Google Scholar] [Publisher link]

[4] Marc Fossi et al., *Symantec Internet Security Threat Report Trends for 2010*, vol. 16, 2011. [Google Scholar] [Publisher link]

[5] Mohamed Ahzam Amanullah et al., “Deep Learning and Big Data Technologies for IoT Security,” *Computer Communications*, vol. 151, pp. 495-517, 2020. [CrossRef] [Google Scholar] [Publisher link]

[6] Sachi Nandan Mohanty et al., “An Efficient Lightweight Integrated Blockchain (ELIB) Model for IoT Security and Privacy,” *Future Generation Computer Systems*, vol. 102, pp. 1027-1037, 2020. [CrossRef] [Google Scholar] [Publisher link]

[7] Charles Wheelus, and Xingquan Zhu, “IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework,” *IoT*, vol. 1, no. 2, pp. 259-285, 2020. [CrossRef] [Google Scholar] [Publisher link]

[8] Bhabendu Kumar Mohanta et al., “Survey on IoT Security: Challenges and Solution Using Machine Learning, Artificial Intelligence and Blockchain Technology,” *Internet of Things*, vol. 11, p. 100227, 2020. [CrossRef] [Google Scholar] [Publisher link]

[9] Madhusanka Liyanage et al., *IoT Security: Advances in Authentication*, John Wiley & Sons, 2020. [Google Scholar] [Publisher link]

[10] José Roldán et al., “Integrating Complex Event Processing and Machine Learning: An Intelligent Architecture for Detecting IoT Security Attacks,” *Expert Systems with Applications*, vol. 149, p. 113251, 2020. [CrossRef] [Google Scholar] [Publisher link]

[11] Rasheed Ahmad, and Izzat Alsmadi, “Machine Learning Approaches to IoT Security: A Systematic Literature Review,” *Internet of Things*, 100365, 2021. [CrossRef] [Google Scholar] [Publisher link]

[12] Omnia Abu Waraga et al., “Design and Implementation of Automated IoT Security Testbed,” *Computers & Security*, vol. 88, p. 101648, 2020. [CrossRef] [Google Scholar] [Publisher link]

[13] Mohammed Ali Al-Garadi et al., “A Survey of Machine and Deep Learning Methods for Internet of Things (Iot) Security,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, 2020. [CrossRef] [Google Scholar] [Publisher link]

[14] Fatima Hussain et al., “Machine Learning in IoT Security: Current Solutions and Future Challenges,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, 2020. [CrossRef] [Google Scholar] [Publisher link]

[15] Abdullah Al Hayajneh, Md Zakirul Alam Bhuiyan, and andIan McAndrew, “Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN),” *Computers*, vol. 9, no. 1, p. 8, 2020. [CrossRef] [Google Scholar] [Publisher link] https://doi.org/10.3390/computers9010008

[16] Hichem Mrabet et al., “A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis,” *Sensors*, vol. 20, no. 13, p. 3625, 2020. [CrossRef] [Google Scholar] [Publisher link]

[17] Lerina Aversano et al., “A Systematic Review on Deep Learning Approaches for IoT Security,” *Computer Science Review*, vol. 40, p. 100389, 2021. [CrossRef] [Google Scholar] [Publisher link]

[18] Chandrasegar Thirumalai, Senthilkumar Mohan, and Gautam Srivastava, “An Efficient Public Key Secure Scheme for Cloud and IoT Security,” *Computer Communications*, vol. 150, pp. 634-643, 2020. [CrossRef] [Google Scholar] [Publisher link]

[19] Shahid Mahmood, Amin Ullah, and Anas Khalid Kayani, “Fog Computing Trust based Architecture for Internet of Things Devices,” *International Journal of Computing and Communication Networks*, vol. 1, no. 1, pp. 18-25, 2019. [Google Scholar] [Publisher link]

[20] Pramod Pavithran et al., “A Novel Cryptosystem Based on DNA Cryptography and Randomly Generated Mealy Machine,” *Computers & Security*, vol. 104, p. 102160, 2021. [CrossRef] [Google Scholar] [Publisher link]

[21] Prema T. Akkasaligar, and Sumangala Biradar, “Selective Medical Image Encryption Using DNA Cryptography,” *Information Security Journal: A Global Perspective*, vol. 29, no. 2, pp. 91-101, 2020. [CrossRef] [Google Scholar] [Publisher link]

[22] Anupam Das, Shikhar Kumar Sarma, and Shrutimala Deka, “Data Security with DNA Cryptography,” *Transactions on Engineering Technologies, Springer, Singapore*, pp. 159-173, 2021. [CrossRef] [Google Scholar] [Publisher link]

[23] Khaled Salah Mohamed, “New Trends in Cryptography: Quantum, Blockchain, Lightweight, Chaotic, and DNA Cryptography,” *New Frontiers in Cryptography, Springer, Cham*, pp. 65-87, 2020. [CrossRef] [Google Scholar] [Publisher link]

[24] Andrea Ceccanti, Enrico Vianello, and Francesco Giacomini, “Beyond X. 509: Token-Based Authentication and Authorization in Practice,” *EPJ Web of Conferences,* EDP Sciences, vol. 245, p. 03021, 2020. [CrossRef] [Google Scholar] [Publisher link]

[25] Jiaxin Li, Zhaoxin Zhang, and Changyong Guo, “Machine Learning-Based Malicious X.509 Certificates’ Detection,” *Applied Sciences*, vol. 11, no. 5, p. 2164, 2021. [CrossRef] [Google Scholar] [Publisher link] https://doi.org/10.3390/app11052164

[26] Naser Peiravian, and Xingquan Zhu, “Machine Learning for Android Malware Detection Using Permission and API Calls,” *2013 IEEE 25th International Conference on Tools with Artificial Intelligence, IEEE,* pp. 300-305, 2013. [CrossRef] [Google Scholar] [Publisher link]

[27] Mukrimah Nawir et al., “Internet of Things (IoT): Taxonomy of Security Attacks,” *2016 3rd International Conference on Electronic Design (ICED), IEEE,* pp. 321-326, 2016. [CrossRef] [Google Scholar] [Publisher link]

[28] S. Durga, Rishabh Nag, and Esther Daniel, “Survey on Machine Learning and Deep Learning Algorithms Used in Internet of Things (Iot) Healthcare,” *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), IEEE*, pp. 1018-1022, 2019. [CrossRef] [Google Scholar] [Publisher link]

[29] Jyoti Kansari, Avinash Dhole, and Yogesh Rathore, "A Survey on Block Cipher and Chaotic Based Encryption Techniques," *International Journal of Computer Trends and Technology*, vol. 69, no. 3, pp. 52-59, 2021. [CrossRef] [Publisher link]

[30] Yair Meidan et al., “Detection of Unauthorized IoT Devices Using Machine Learning Techniques,” *arXiv preprint arXiv:1709.04647,* 2016. [CrossRef] [Google Scholar] [Publisher link]

[31] Rohan Doshi, Noah Apthorpe, and Nick Feamster, “Machine Learning DDos Detection for Consumer Internet of Things Devices,” *2018 IEEE Security and Privacy Workshops (SPW), IEEE*, pp. 29-35, 2018. [CrossRef] [Google Scholar] [Publisher link]

[32] Markus Miettinen et al., “IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT,” *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), IEEE,* pp. 2177-2184, 2017. [CrossRef] [Google Scholar] [Publisher link]

[33] Robert Moskovitch et al., “Improving the Detection of Unknown Computer Worms Activity Using Active Learning,” *Annual Conference on Artificial Intelligence*, *Springer,* Berlin, Heidelberg, pp. 489-493, 2007. [CrossRef] [Google Scholar] [Publisher link]

[34] Ivana Damgård et al., “Fast Threshold ECDSA with Honest Majority,” *International Conference on Security and Cryptography for Networks, Springer,* Cham, pp. 382-400, 2020. [CrossRef] [Google Scholar] [Publisher link]

[35] Huiyi Han, Zhiyi Qu, and Weiwei Kang, "A Login Strategy using Fingerprint Verification," *SSRG International Journal of Computer Science and Engineering*, vol. 2, no. 7, pp. 35-39, 2015. [CrossRef] [Publisher link]

[36] Hiran V. Nath, and Babu M. Mehtre, “Static Malware Analysis Using Machine Learning Methods,” *International Conference on Security in Computer Networks and Distributed Systems, Springer,* Berlin, Heidelberg, pp. 440-450, 2014. [CrossRef] [Google Scholar] [Publisher link]

[37] Vikas Hassija et al., “A Survey on Iot Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721-82743, 2019. [CrossRef] [Google Scholar] [Publisher link]

[38] Kawtar Bouzoubaa, Youssef Taher, and Benayad Nsiri, “DOS-DDOS Attacks Predicting: Performance Comparison of the Main Feature Selection Strategies,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 1, pp. 299-312, 2022. [CrossRef] [Google Scholar] [Publisher link]

[39] Enrique Lee Huamaní et al., “Design of an IoT Prototype for the Prevention of Robberies in the Young Areas of Lima,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, pp. 111-118, 2022. [CrossRef] [Google Scholar] [Publisher link]

[40] N. Krishnaraj, and S. Sangeetha, “A Study of Data Privacy in Internet of Things Using Privacy Preserving Techniques with its Management,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 3, pp. 54-65, 2022. [CrossRef] [Google Scholar] [Publisher link]

[41] Suyel Namasudra, “A Secure Cryptosystem Using DNA Cryptography and DNA Steganography for the Cloud-Based IoT Infrastructure,” *Computers and Electrical Engineering*, vol. 104, p. 108426, 2022. [CrossRef] [Google Scholar] [Publisher link]

[42] Pratyusa Mukherjee et al., "Emerging DNA Cryptography-Based Encryption Schemes: A Review," *International Journal of Information and Computer Security*, vol. 20, no. 1-2, pp. 27-47, 2023. [CrossRef] [Google Scholar] [Publisher link]

[43] M. Indrasena Reddy, A.P. Siva Kumar, and K. Subba Reddy, "A Secured Cryptographic System Based on DNA and a Hybrid Key Generation Approach," *Biosystems*, vol. 197, p. 104207, 2020. [CrossRef] [Google Scholar] [Publisher link]

[44] Lalit Mohan Gupta, Hitendra Garg, and Abdus Samad, "A Secure Data Transfer Approach with an Efficient Key Management Over Cloud," *International Journal of Information Technology and Web Engineering (IJITWE)*, vol. 17, no. 1, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher link]

[45] CH.Jayanthi, and V.Srinivas, "Mathematical Modelling for Cryptography using Laplace Transform," *International Journal of Mathematics Trends and Technology*, vol. 65, no. 2, pp. 10-15, 2019. [CrossRef] [Google Scholar] [Publisher link]

[46] Liang Xiao et al., "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, 2018. [CrossRef] [Google Scholar] [Publisher link]

[47] Stanislav Ponomarev, and Travis Atkison, "Industrial Control System Network Intrusion Detection by Telemetry Analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 252-260, 2015. [CrossRef] [Google Scholar] [Publisher link]