OCTOPUS++: AN ENHANCED MUTUAL AUTHENTICATION SECURITY PROTOCOL AND LIGHTWEIGHT ENCRYPTION AND DECRYPTION ALGORITHM BASED ON DNA IN FOG COMPUTING

GOHAR RAHMAN

A thesis submitted in
fulfilment of the requirement for the award of the
Doctor of Philosophy in Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

JULY 2023

DEDICATION

To my beloved Parents

ACKNOWLEDGEMENT

In the name of Allah, I attest that there is no deity but Allah, and that Hazrat Muhammad (PBUH) is His last prophet, who built humanity's advancement on knowledge. For providing me with the talented teachers, lucrative possibilities, and assistance for arranging and carrying out this research project, I am unable to adequately convey my appreciation to Allah Almighty in literary form.

First and foremost, I would like to extend my profound gratitude to Dr Chuah Chai Wen, my deserving, caring, and compassionate supervisor, for her sincere guidance and professional advice during the entirety of my research project. It's fantastic and important to recognize her quick ability to spot issues and provide solutions. My capability of critically analyzing logical methods has been significantly improved by her nice attitude and manner of discussions. She has been an inspiration and a mentor to me over the course of my study endeavour. My plans for my studies have been significantly influenced by her opinions and concepts. She genuinely helped me out in whatever way she could. Without her steadfast assistance, I would not have been able to accomplish my goal. I was able to do my entire assignment thanks to her abilities.

I will always remember the academic resources and research-focused environment provided by the Faculty of Computer Science and Information Technology (FSKTM) and Universiti Tun Hussein Onn Malaysia (UTHM). It is amazing to see how diligently UTHM staff and management work to give all modern amenities and cutting-edge instruction across the board. We were able to learn Information Technology (IT) in a research-focused environment because to their sincere efforts and attitude. Likewise, I would like to express my gratitude to Universiti Tun Hussein Onn Malaysia and the Malaysian Ministry of Higher Education (MOHE) for funding this study via the Fundamental Research Grant Scheme Vot No FRGS/1/2020/ICT03/UTHM/03/5.

Last but not least, it is a depressing truth that during this protracted journey I did not have enough time to serve my old great DAJI (my father) and Abai (my mother), but their prayers stayed with me entirely and yet still stay with me. Throughout my existence on this world, their sincere prayers, advice, support, love, and care were of immense help to me. My parents have always served as my primary source of inspiration and guidance. I applaud them because I could not have accomplished my academic goals without their selfless and unwavering assistance. They are the subject of this investigation. My brothers, sisters, and other family members deserve praise as well for their continuous encouragement and support.

Thanks in particular to all of my friends who have motivated me in any way morally, intellectually, spiritually, or in any other way. I am also fortunate of all of my UTHM friends who never let me feel alone during my protracted stay abroad by offering me their counsel, encouragement, support, and wonderful company. Thank you very much.

Gohar Rahman ,UTHM, Malaysia

ABSTRACT

The Internet of Things (IoT) envisions a world wherein everyday objects may connect to the internet and exchange data, analyse, store, and gather data from their environment and efficiently mediate on it. Fog computing, closer to the IoT, is formulated in data processing, filtering, aggregating, and storing. In fog IoT network one of the main challenges is security. The existing security solutions are based on modern cryptography algorithms are computationally complex which causes the fog IoT network to slow down. Therefore, in fog IoT the operations must be lightweight and secure. The security considerations include attacks, especially Man in the Middle attack (MitM), challenges, requirements, and existing solutions that are deeply analyzed and reviewed. Hence, omega network key generation based on deoxyribonucleic acid (ONDNA) is proposed, which provides lightweight encryption and decryption in fog computing. The security level of ONDNA is tested using NIST test suite. ONDNA passes all the 17 recommended NIST Test Suite tests. Next, we proposed a modified security protocol based on ONDNA and hash message authentication code with secure hash algorithm 2. The modified protocol is noted as OCTOPUS++. We proved that the OCTOPUS++ provides confidentiality, mutual authentication, and resistance to MitM attack using the widely accepted Burrows Abdi Needham (BAN) logic. The OCTOPUS++ is evaluated in terms of execution time. The average execution time for 20-time execution of OCTOPUS++ is 1.018917 milliseconds. The average execution time for Octopus, LAMAS and Amor is 2.444324, 20.1638 and 14.1152 milliseconds respectively. The results show that the OCTOPUS++ has less execution time than other existing protocols.

ABSTRAK

Internet Benda (IoT) merupakan pengantar yang cekap di mana objek harian bersambung ke Internet, data persekitaran objek dikumpul, disimpan dan data dianalisa. Pengkomputeran kabus merupakan pengkomputeran yang lebih dekat dengan IoT yang membolehkan pemprosesan data, penapisan, pengagregatan dan penyimpanan data. Keselamatan merupakan salah satu cabaran utama dalam rangkaian IoT kabus. Penyelesaian yang sedia ada adalah berdasarkan kepada pengiraan algoritma kriptografi moden yang kompleks, ini juga merupakan penyebab rangkaian IoT kabus menjadi perlahan. Oleh itu, operasi IoT kabus mestilah ringan dan juga selamat. Keselamatan dalam pertimbangan termasuk penyerangan terutamanya serangan *Man in the Middle* (MitM), cabaran, keperluan dan penyelesaian sedia ada dianalisi dan disemak secara mendalam. Oleh itu, rangkaian omega penjanaan kunci berasaskan asid deoksiribonukleik (ONDNA) di cadangkan, di mana penyulitan dan penyahsulitannya adalah ringan dalam pengkomputeran kabus. Tahap keselamatan ONDNA diuji dengan menggunakan ujian NIST. ONDNA lulus kesemua 17 ujian NIST yang disyorkan. Seterusnya, kami mencadangkan satu penambahbaikan protokol keselamatan berdasarkan ONDNA dan kod pengesahan mesej dengan algoritma hash. Protokol yang diubah suai ini dikenali sebagai OCTOPUS++. Kami membuktikan bahawa OCTOPUS++ menyediakan kerahsiaan dan pengesahan bersama serta penentangan terhadap serangan MitM menggunakan logik *Burrows Abdi Needham* (BAN) yang diterima secara meluas. OCTOPUS++ dinilai dari segi masa pelaksanaan. Masa pelaksanaan diukur dalam milisaat. Purata masa 20 kali pelaksanaan untuk OCTOPUS++ adalah 1.018917 milisaat. Purata masa 20 kali pelaksanaan untuk Octopus, LAMAS dan Amor adalah 2.444324milisaat, 20.1638 dan 14.1152 milisaat. Keputusan menunjukkan bahawa masa pelaksanaan OCTOPUS++ adalah kurang berbanding protokol yang sedia ada.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PUBLICATIONS

i. Rahman, G., & Wen, C. C. (2018). Fog computing, applications, security and challenges, review. Int. J. Eng. Technol, 7(3), 1615-1621(Scopus Indexed)

ii. Rahman, G., & Wen, C. C. (2019). Man in the Middle Attack Prevention for edge-fog, mutual authentication scheme. International Journal of Recent Technology and Engineering (IJRTE), 8(2s2)(Scopus Indexed)

iii. Rahman, G., & Wen, C. C. (2019). Mutual authentication security scheme in fog computing. International Journal of Advanced Computer Science and Applications, 10(11)(Web of science(WOS) and Scopus Indexed)

iv. Rahman, Gohar, and Chuah Chai Wen. 2022. "Omega Network Pseudorandom Key Generation Based on DNA Cryptography" Applied Sciences 12, no. 16: 8141(ISI and Scopus Indexed: IF=2.838)

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Internet of Things (IoT) is the latest technology that connects and communicates interrelated intelligent objects without human involvement (Yousefpour *et al.*, 2017). The interrelated intelligent objects can be smartphones, cameras, sensors, and portable devices. It is expected that by 2025, tens of billions of smart intelligent IoT devices will invade the world (Hu *et al.*, 2017; Gill & Singh, 2021). Many IoT applications are being structured in different industries including smart city, smart grid, and home support, also in healthcare services, inventory systems, and transportation (Silva *et al.*, 2017). However, to ensure effective communication for these interrelated intelligent objects, it is necessary to ensure the network is of high speed and instant response time. Cloud computing is the existing technology that enables applications with large storage and processing power (Yousefpour *et al.*, 2017; Deng *et al.*, 2021).

Cloud computing allows data access to an internet connection (Ghobaei *et al.*, 2019). A typical IoT cloud architecture works in three phases. IoT devices reside in the first phase, where sensors collect the information and forward the collected information to the cloud servers. In the second phase, cloud servers analyze the information received. In the third phase, the cloud servers process the information and send it back to the IoT devices. In this case, cloud computing compromises high latency, security, and privacy of data (Abubaker *et al.*, 2017; Ni *et al.*, 2018). One of the limitations of cloud computing is that it cannot provide low latency and real-time processing for connected smart devices as cloud computing is located far from the interrelated intelligent devices (Zhang *et al.*, 2010; Bonomi *et al.*, 2012; Libawy *et al.*, 2019). Therefore, fog computing was invented to overcome the limitations of cloud computing (Malik *et al.*, 2021), that provide low latency and location awareness and can improve the quality of services (QoS) for real-time applications (Stojmenovic & Wen, 2014).

Fog computing is a decentralized architecture that processes data between IoT devices and cloud servers. This computing paradigm brings the services of cloud computing closer to the edge devices. The edge devices, such as switches, routers, and gateways, act as a computing nodes along with the cloud data centre (Nath *et al.*, 2018). Compared to cloud computing, fog computing computations offers better results: location awareness, geographical accessibility, low latency, and mobility support. The fog computing nodes are located near the IoT devices (Ai *et al.*, 2018).

Fog computing provides data processing and storage services to IoT users. In fog computing, the processed information is transmitted and stored locally on fog devices instead of being sent to the cloud (Ekanayake *et al.*, 2018). The architecture of fog computing consists of three layers as well. The first layer contains IoT devices such as sensors, wearable actuators, smartphones, and smartwatches. The second layer, the middle layer, consists of fog nodes where the computation is performed in real-time. The last layer includes the cloud server, where the data is stored for future use (Verma *et al.*, 2016). Fog computing is seen as an extension of cloud computing, and the security problems in the cloud are inherited from fog computing. As fog computing is decentralized, the same methods applied to cloud computing did not apply to fog computing (Praveen, 2016; Abbasi & Shah, 2017). When a user opens their resources in fog computing, the attackers may easily come and attack the fog nodes (Sun *et al.*, 2018). One critical malicious attack is Man in the Middle attack (MitM) (Li *et al.*,2017; Ni *et al.*, 2018). In this attack, the attacker is passed out through a malicious inner user between two computers, secretly relays, and pretending to be legitimate (Wang *et al.*, 2015).

MitM is categorized as passive and active attacks, also known as eavesdropping and manipulation. Eavesdropping is a passive attack as the attacker is merely concerned about the transmitted information. In a manipulation attack, the attacker changes the data sent to it and pretends it as the original sender. Detecting and preventig MitM attacks is essential to dealing with fog computing (Ekanayake *et al.*, 2018). The fog architecture is typically analogous to a MitM attack, as the fog node is intermediate in the cloud and IoT devices, allowing the attacker to easily interfere. For example, nodes dramatically transform personal data , such as medical history of a patient, prescription, and health status of a person. Such information can be terrible in the wrong hands (Khan *et al.*, 2017). This indicates that a strong cryptosystem is required to enhance the security and privacy of fog computing. Authentication and encryption are the most important functions of each cryptosystem because fog-to-things computing inherits threats from the traditional internet. After all, it is connected.

Ibrahim (2016) designed a protocol, Octopus in fog computing, which applies the advanced encryption standard (AES) and hash function to provide mutual authentication and confidentiality services to fog users. However, the Octopus protocol has a significant drawback which it did not consider the anonymity of fog users. The identity of the fog users is transmitted publically. Hence, it is vulnerable to a MitM attack. Other work designed by Amor *et al.* (2017) and LAMAS protocol designed by Mariam *et al.* (2022) achieved mutual authentication and confidential communication between fog users and fog servers. Their work is based on an elliptic curve cryptography asymmetric algorithm which required high computation costs for fog users and fog servers.

This research aimed to focus on the confidentiality aspect of fog computing and to develop a new encryption method to assure confidentiality by using lightweight deoxyribonucleic acid (DNA) cryptography. DNA cryptography is the latest advancement in cryptographic approaches, in which the natural process of DNA synthesis explains that DNA can be used as a carrier of information and how the current science of biotechnology can convert plaintext into ciphertext (Kumaraguru &Chakravarthy, 2018; Satir & Kendirli, 2022). The primary aim of DNA cryptography is to provide greater secrecy than traditional cryptography by combining biological and computational properties (Zhang *et al.*, 2018). DNA cryptography uses DNA computing, while DNA computing holds several benefits, such as high parallelism, lower power consumption, and massive data storage. Based on these characteristics, DNA cryptography has a unique advantage in massively parallel data encryption applications with less real-time demand, secure data storage, and information hiding (Zhang *et al.*, 2016). This research contributed to fog computing, a new omega network DNA key generation design used to encrypt and decrypt the information between fog users and servers. The proposed key is pseudorandom, which passess all the NIST Test Suite recommended tests. Next, in this research, a secure modified security protocol OCTOPUS++ based on ONDNA is proposed, which is to overcome the security problem in the existing security protocol Octopus (Ibrahim, 2016). The security proof is carried out for the OCTOPUS++ protocol by using BAN logic (Sierra *et al.*, 2004). The OCTOPUS++ provided confidential and mutual authentication services and resistance to the MitM attack.

1.2 Problem Statement

Fog computing has extended cloud computing to run on IoT data at the network edge (Rashid &Ravindran, 2019). This leads to a greater security risk for the fog networks because fog or IoT computing inherits the threats of the traditional internet by adding a large numbers of devices and service providers, which is connected to the internet. Fog or IoT computing inherits threats from traditional internet, hence secure fog network is significantly important to design optimal fog networks (Yi *et al.*, 2015). Moreover, the data transmission over an insecure channel such as wireless should be guarded by encryption mechanisms. However, confidential communication between fog and IoT is a critical requirement because the underlying wireless environment is less protected than a wired network. Confidentiality is the idea that prevents unauthorized persons, resources, or processes from accessing data or information (Diro *et al.,* 2018). Most existing techniques use modern cryptographic methods and techniques such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) for confidential data transport, and Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) for encryption and digital signatures. Although these algorithms are robust to meet security requirements, however they are not directly suited for resource constrained fog or IoT networks as they require high resource usage and are computationally complex (Gohany & Almotairi, 2019).

Three security protocols are presented for mutual authentication and encryption between fog IoT cloud architecture. In the first protocol, Octopus (Ibrahim, 2016) did not protect the user's anonymity.The identity of the fog user is publically transmitted through the common channel. Thus, the adversary intercepts the identity and can easily access the session key. Hence, in this protocol, the MitM attack occurs. The second protocol designed by Amor *et al.* (2017), and the third protocol LAMAS designed by Mariam *et al.* (2022) are based on a public key cryptosystem which is not lightweight enough because a public key cryptosystem has expensive computations that are considered impractical in fog end-user equipment due to the inherent characteristics of the end user design, for instance, limited memory, processing, and battery power (Haroon *et al.,* 2016; Albakri *et al.,* 2018).

This motivated us to develope a new lightweight omega network DNA key generator, that ensures data protection in fog or IoT environments and is well suited for IoT fog computing environment. The omega network uses the concept of the central dogma of microbiology DNA and RNA properties, including DNA replication for DNA and the transcription process for RNA. The existing protocol Octopus has been extended and brought a secure modified security protocol OCTOPUS++, which provides the best security level and resistance to MitM attack in a fog IoT environment.

1.3 Objective

The objective of this research is as follow:

i) To design omega network pseudorandom key and DNA generation based on DNA cryptograpy for fog computing.
ii) To implement the proposed lightweight encryption in fog computing.
iii) To validate/evaluate the lightweight cipher using Burrows Abdi Needham (BAN) logic, NIST and execution time in fog computing.

1.4 Scope of The Research

Confidentiality and anonymity in fog computing is an open research challenge. This research focuses on how confidential and anonymous communication between a fog node and a fog server can be established and what advantages confidentiality can provide in fog computing. Preventing MitM attack in fog computing is a prominent challenge. The proposed solution aims to protect fog computing from this attack. BAN logic is used to prove that the OCTOPUS++ protocol of fog computing is secured.

Next, by utilizing the benefits of DNA cryptography, key generation and encryption algorithm based on DNA cryptography are presented. The proposed algorithm provides strong, lightweight encryption methods and a key generation that fit for constrained devices in a fog IoT environment. The pseudorandomness of the ONDNA is tested by using the NIST test suite.

1.5 Motivation

Fog computing is still an open research area because of its infancy stage. The motivation for developing a secure fog environment for IoT-based applications services comes from the ongoing challenges associated with fog computing (Al-khafajiy *et al.,* 2018; Abdulkareem *et al.,* 2019; Habibi *et al.*, 2020). Therefore, bringing computing resources to network edges efficiently and securely is a hot topic among researchers (Wang *et al.*, 2017; Khafajiy *et al.*, 2019).

Fog nodes are installed at the network's edge, and they lack the resources and processing power compared to cloud nodes. As a result, fog nodes can be more accessible, dependent on network configuration due to physical location, which raises the risk of attacks. Thus, avoiding fraudulent or malicious fog nodes is still an open challenge (Puthal *et al.*, 2016; Puthal *et al.*, 2019). Thus, these challenges motivated us to design a secure protocol to fulfil all the security services in the fog computing environment.

Another significant challenge is choosing ciphers for the encryption process to avoid cyber threats. Cryptography is commonly performed with symmetric and asymmetric algorithms in IoT fog environments. Asymmetric algorithm like AES and DES while asymmetric algorithm RSA and ECC. These cryptographic algorithms require a lot of processing power which is computationally complex in a fog environment (Rahman *et al.*, 2019).

The above mentioned challenges raise the motivation to introduce a new field in fog computing, which is best known for strong security, large data storage, and being less computationally complex. This new domain is a term for DNA cryptography. DNA cryptography consists of genetics and bimolecular computation and is one of the latest directions in cryptography. Genetic material such as DNA can be used as a massive storage capacity. A gram of DNA molecules consists of 1021 DNA bases, nearly 108 tera-byte (Anwar*et al.,* 2015; Cherillath & Mohammed, 2018; Mandrita & Kumar, 2019). This idea is inspired by the fact that DNA is a natural carrier of information, which is encoded by a 4-letter alphabet: A, C, G, and T. This alphabet can be easily transposed into the binary alphabet A, 00, C, 01, G, 10, T, 11. Therefore DNA can be used as a storage media for any kind of information (Biswas *et al.*, 2017; Kalsi *et al.*, 2018).

DNA cryptography has a unique advantage in massively parallel lightweight data encryption applications with less real-time demand, secure data storage, authentication, digital signature, and information hiding (Zhang*et al.,* 2016, Shah & Pippal, 2021). This has motivated us to apply DNA cryptography in fog computing. The concept of the central dogma of microbiology DNA and RNA properties, including DNA replication for DNA and transcription process for RNA, are exploited to design a strong DNA pseudorandom key and encryption and decryption algorithm.

1.6 Thesis Outline

This chapter presents a brief introduction with background knowledge of the IoT, fog computing, cloud computing, the problem statement, objectives, and scope of this research study. The rest of the chapters are organized as follows:

Chapter 2 discusses the basic concepts related to resource constrained IoT devices and fog computing. This chapter also explores the standard theoretical concepts and the operational mechanisms of various security protocols used to solve the security privacy, and anonymity issues in fog computing and other various domains. This chapter also discusses the emerging field in the history of cryptography which is DNA cryptography. The central dogma of DNA presented in this chapter are transcription, translation, and complementary rules. This chapter describes the techniques used throughout this research to achieve its aims and objective. BAN logic, message authentication code (MAC), digital signature algorithm, complementary rules, mRNA rules, DNA XORing rules, and NIST Test Suite.

Chapter 3 consists of the proposed methodology and research framework. This chapter presents the overall research activity which has been carried out.

Chapter 4 consists OCTOPUS++ protocol. The OCTOPUS++ is based on ONDNA and hash message authentication code with secure hash algorithm 2. The experiment execution time setup of OCTOPUS++ and the NIST Test Suite setup is also presented in this chapter.

Chapter 5 presents results and discussions of the NIST Test Suite results and the formal security proof of the OCTOPUS++ based on BAN logic. The execution time comparison of the OCTOPUS++ with the existing security protocols is also part of this chapter.

Chapter 6 concludes the research work with a short description of the accomplished objectives, contributions of the research work, and future directions.

REFERENCES

Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile Edge Computing: A Survey. *IEEE Internet of Things Journal*, 5(1), 450–465.

Abbasi, B. Z., & Shah, M. A. (2017). Fog Computing: Security Issues, Solutions and Robust Practices. *In 2017 23rd international conference on automation and computing (ICAC)*, 1-6.

Abdulkareem, K. H., Mohammed, M. A., Gunasekaran, S. S., Al-Mhiqani, M. N., Mutlag, A. A., Mostafa, S. A., Ali, N. S., & Ibrahim, D. A. (2019). A Review of Fog Computing and Machine Learning: Concepts, Applications, Challenges, and Open Issues. *IEEE Access, 7*, 153123–153140.

Abubaker, N., Dervishi, L., & Ayday, E. (2017). Privacy-Preserving Fog Computing Paradigm. *In 2017 IEEE Conference on Communications and Network Security (CNS)*, 502-509.

Ai, Y., Peng, M., & Zhang, K. (2018). Edge Computing Technologies for Internet of Things: a primer. *Digital Communications and Networks*, 4(2), 77–86.

Al - Wattar, A. H. S., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). Generating a New S-Box Inspired by Biological DNA. *International Journal of Computer Science and Application*, 4(1), 32–42.

Al Hamid, H. A., Rahman, S. M. M., Shamim Hossain, M., Almogren, A., & Alamri, A. (2017). A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography. *IEEE Access*, 5, 22313–22328.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things Security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28.

AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile Cloud Computing Models Security Issues: A systematic Review. *Journal of Network and Computer Applications*, 190(5), 1-17.

Alamer, A. (2021). Security and Privacy-awareness in a Software-Defined Fog Computing Network for the Internet of Things. *Optical Switching and Networking*, 41(3), 1-10.

Alawad, F., & Kraemer, F. A. (2022). Value of information in wireless sensor network applications and the IoT: A review. IEEE Sensors Journal.

Alazeb, A., Panda, B., Almakdi, S., & Alshehri, M. (2021). Data Integrity Preservation Schemes in Smart Healthcare Systems That Use Fog computing Distribution. *Electronics,* 10(11), 1-27.

Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P. (2018). Novel Hybrid Encryption Algorithm Based on AES, RSA, and Twofish for Bluetooth Encryption. *Journal of Information Security*, 9(2), 168–176.

Albakri, A., Maddumala, M., & Harn, L. (2018, August). Hierarchical Polynomial-Based Key Management Scheme in Fog Computing. *In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, 1593-1597.

Al-gohany, N. A., & Almotairi, S. (2019). Comparative Study of Database Security In Cloud Computing Using AES and DES Encryption Algorithms. *Journal of Information Security and Cybercrimes Research*, 2(1), 102–109.

Ali, A. I. (2015). Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network. *International Journal of Embedded Systems and Applications*, *5*(2), 15–29.

Al-Janabi, S., Al-Khateeb, B., & Abd, A. (2017). Intelligent Techniques in Cryptanalysis: Review and Future Directions. *UHD Journal of Science and Technology*, 1(1), 1–10.

Al-Khafajiy, M., Baker, T., Al-Libawy, H., Waraich, A., Chalmers, C., & Alfandi, O. (2019). Fog Computing Framework for Internet of Things Applications. *Proceedings International Conference on Developments in ESystems Engineering*, 71–77.

Al-Khafajiy, M., Baker, T., Waraich, A., Al-Jumeily, D., & Hussain, A. (2019). IoT Fog Optimal Workload via Fog Offloading. *Proceedings 11th IEEE/ACM International Conference on Utility and Cloud Computing Companion, UCC*

Companion, Zurich, Switzerland, 349–352.

Al-Khafajiy, M., Webster, L., Baker, T., & Waraich, A. (2018). Towards Fog Driven IoT Healthcare: Challenges and Framework of Fog Computing in Healthcare. *In Proceedings of the 2nd international conference on future networks and distributed systems*, 1-7.

Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS, *Sensors*, 22(4), 1448.

Alotaibi, A., Barnawi, A., & Buhari, M. (2017). Attribute-Based Secure Data Sharing with Efficient Revocation in Fog Computing. *Journal of Information Security*, *8*(3), 203–222.

Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017a). An Attribute-Based Encryption Scheme to Secure Fog Communications. *IEEE Access*, *5*(c), 9131–9138.

Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017b). An Attribute-Based Encryption Scheme to Secure Fog Communications. *IEEE Access*, 5, 9131–9138.

Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al-Ahmad, A. (2021). Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy*, *4*(2), 1–26.

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Kumar, N. (2018). A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Generation Computer Systems*, *80*, 483-495.

Amor, A. B., Abid, M., & Meddeb, A. (2017). A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment. *In 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA),* 1225-1231.

Anwar, T., Kumar, A., & Paul, S. (2015). DNA Cryptography Based on Symmetric Key Exchange. *International Journal of Engineering and Technology (IJET),* 7(3), 938–950.

Ashjaei, M., & Bengtsson, M. (2017, December). Enhancing Smart Maintenance Management using Fog Computing Technology. *In 2017 IEEE International Conference on Industrial Engineering and Engineering Management*

(IEEM),1561-1565.

Atassi, M. Z. (n.d.). *Protein Reviews Series Editor*. www.springer.com/series/6876

Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog Computing and the Internet of Things: A Review. *Big Data and Cognitive Computing*, 2(2), 1–18.

Auday H. Saeed Al-Wattar, Ramlan Mahmod, Z. A. Z. &, & Nur Izura Udzir. (2015). Review of Dna and Pseudo Dna Cryptography. *International Journal of Computer Science and Engineering (IJCSE)*, 4(4), 65–76.

Azad, S., & Pathan, A. S. K. (Eds.) (2014). Practical cryptography: algorithms and implementations using C++. CRC Press.

Bachiega Jr, J., Costa, B., & Araujo, A. P. (2022). Computational Perspective of the Fog Node. *arXiv preprint arXiv*:2203–2214.

Bae, W. il, & Kwak, J. (2020). Smart Card-Based Secure Authentication Protocol in Multi-Server IoT Environment. *Multimedia Tools and Applications*, *79*(23), 15793–15811.

Bahrami, P. N., Javadi, H. H. S., Dargahi, T., Dehghantanha, A., & Choo, K. K. R. (2019). A Hierarchical Key Pre-Distribution Scheme for Fog Networks. *Concurrency Computation* , 31(22), 1–14.

Bangare, M. L., Bangare, P. M., Apare, R. S., & Bangare, S. L. (2021). Fog Computing Based Security of IoT Application. Design Engineering,7, 7542-7549.

Baranwal, G., & Vidyarthi, D. P. (2021). FONS: A Fog Orchestrator Node Selection Model to Improve Application Placement in Fog Computing. *Journal of Supercomputing*, *77*(9), 10562–10589.

Basu, S., Karuppiah, M., Nasipuri, M., Halder, A. K., & Radhakrishnan, N. (2019). Bio-Inspired Cryptosystem with DNA Cryptography and Neural networks. *Journal of Systems Architecture*, 94(2), 24–31.

Bellare, M., Canetti, R., & Krawczyk, H. (1996). Message Authentication Using Hash Functions—the HMAC Construction. *RSA Laboratories' CryptoBytes*, 2(1), 1–5.

Bellavista, P., Berrocal, J., Corradi, A., Das, S. K., Foschini, L., & Zanni, A. (2019). A Survey on Fog Computing for the Internet of Things. *Pervasive and Mobile Computing*, 52, 71–99.

Biswas, M. R., Alam, K. M. R., Akber, A., & Morimoto, Y. (2017, December). A

DNA Cryptographic Technique Based on Dynamic DNA Encoding and Asymmetric Cryptosystem. *In 2017 4th International Conference on Networking, Systems and Security (NSysS)*,1-8.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog Computing and its Role in the Internet of Things. *In Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 13-16.

Bormann, C., Ersue, M., & Keranen, A. (2014). Terminology for constrained-node networks (No. rfc7228).

Burrows, M., Abadi, M., & Needham, R. (1990). A Logic of Authentication. *ACM Transactions on Computer Systems (TOCS)*, 8(1), 18-36.

Cardelli, L. (2013). Two-Domain DNA Strand Displacement. *Mathematical Structures in Computer Science*, 23(2), 247–271.

Chen, S. Y., LIU, Y. L., LIN, C. L., LI, T., & DONG, Y. Q. (2022). Lightweight Verifiable Group Authentication Scheme for the Internet of Things. *ACTA ELECTONICA SINICA*, 50(4), 990.

Cherillath Sukumaran, S., & Mohammed, M. (2018). DNA Cryptography for Secure Data Storage in Cloud. *International Journal of Network Security*, 20(3), 447–454.

Cheung, D., Maslov, D., Mathew, J., & Pradhan, D. K. (2008). On the Design and Optimization of a Quantum Polynomial-time Attack on Elliptic Curve Cryptography. *In Workshop on Quantum Computation, Communication, and Cryptography*, 96-104.

Cui, G., Li, C., Li, H., & Li, X. (2009). DNA Computing and its Application to Information Security Field. *5th International Conference on Natural Computation, ICNC 2009*, *6*(C), 148–152.

Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing*, 13(2), 241-251.

Dale Liu, Caceres, M., Robichaux, T., Forte, D. V., Seagren, E. S., Ganger, D. L., Smith, B., Jayawickrama, W., Stokes, C., & Jan Kanclirz, J. (2009). Chapter 3 - An Introduction To Cryptography. *Next Generation SSH2 Implementation*, 41–64.

Dammak, B., Turki, M., Cheikhrouhou, S., Baklouti, M., Mars, R., & Dhahbi, A. (2022). Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring. *Sensors, 22*(4), 1497.

Dar, A. R., & Ravindran, D. (2019). Fog Computing: An Extended Version of Cloud Computing. *Int. J. Mod. Electron. Commun. Eng, 7, 40-45.*

David Solomon Raju, T. S. R. (2021). Implementation of Data Security with Wallace Tree Approach Using Elliptical Curve Cryptography on FPGA. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(6), 1546–1553.

Deepa, N. R., & Sivamangai, N. M. (2022). A State-Of-Art Model of Encrypting Medical Image Using DNA Cryptography and Hybrid Chaos Map-2d Zaslavaski Map. *In 2022 6th International Conference on Devices, Circuits and Systems (ICDCS)*, 190-195.

Deng, Q., Goudarzi, M., & Buyya, R. (2021). Fogbus2: a Lightweight and Distributed Container-based Framework for Integration of IoT-Enabled systems with Edge and Cloud Computing. *In Proceedings of the International Workshop on Big Data in Emergent Distributed Environments*, 1-8.

Diro, A. A., Chilamkurti, N., & Kumar, N. (2017). Lightweight Cybersecurity Schemes Using Elliptic Curve Cryptography in Publish-Subscribe fog Computing. *Mobile Networks and Applications*, 22(5), 848–858.

Diro, A. A., Chilamkurti, N., & Nam, Y. (2018). Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication. *IEEE Access*, 6, 26820–26830.

Dixon, H. B. F., Bielka, H., & Cantor, C. R. (1986). Nomenclature Committee for the International Union of Biochemistry (NC-IUB). Nomenclature for Incompletely Specified Bases in Nucleic Acid Sequences. Recommendations 1984. *Nucleic acids research*, 83(1), 4–8.

Dong, M. T., & Zhou, X. (2016). Fog Computing: Comprehensive Approach for Security Data Theft Attack Using Elliptic Curve Cryptography and Decoy Technology. *OALib*, 3(9), 1–14.

Dsouza, C., Ahn, G. J., & Taguinod, M. (2014, August). Policy-Driven Security Management for Fog Computing: Preliminary Framework and a Case Study. *In Proceedings of the 2014 IEEE 15th international conference on information* *reuse and integration*, 16-23.

Ekanayake, B. N. B., Halgamuge, M. N., & Syed, A. (2018). Review: Security and Privacy issues of fog computing for the Internet of Things (IoT). In *Lecture Notes on Data Engineering and Communications Technologies*, 14, 139-174.

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The Internet of Things : New Interoperability, Management and Security Challenges. *International Journal of Network Security & Its Applications*, 8(2), 85–102.

Fakeeh, K. A. (2016). Privacy and security problems in fog computing. *Applied Electronics*, 4(6), 1–7.

Ferguson, P., & Senie, D. (1998). Network Ingress Filtering: Defeating denial of Service Attacks Which Employ IP Source Address Spoofing (No. rfc2267).

Fu, J. S., Liu, Y., Chao, H. C., Bhargava, B. K., & Zhang, Z. J. (2018). Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. *IEEE Transactions on Industrial Informatics*, 14(10), 4519–4528.

Ghobaei-Arani, M., Souri, A., Baker, T., & Hussien, A. (2019). ControCity: An Autonomous Approach for Controlling Elasticity Using Buffer Management in Cloud Computing Environment. *IEEE Access*, 7, 106912–106924.

Gill, M., & Singh, D. (2021). A Comprehensive Study of Simulation Frameworks and Research Directions in Fog computing. *Computer Science Review*, *40*, 100391.

Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., & Leon-Garcia, A. (2020). Fog Computing: A Comprehensive Architectural Survey. *IEEE Access*, 8, 69105–69133.

Hamid, O. K., Abduljabbar, R. B., & Alhyani, N. J. (2020). Fast and Robust Approach For Data Security in Communication Channel Using Pascal Matrix. *Indonesian Journal of Electrical Engineering and Computer Science*, 19(1), 248–256.

Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., & Bentaleb, A. (2019). Enhanced authentication and key management scheme for securing data transmission in the internet of things. Ad Hoc Networks, 94, 101948.

Hardi, S. M., Tarigan, J. T., & Safrina, N. (2018). Hybrid Cryptosystem for Image File Using Elgamal and Double Playfair Cipher Algorithm. *Journal of Physics: Conference Series*, 978(1), 2034-2043.

Hasan, H. A. A., Mohammed, S. M., & Ameer, N. H. A. (2021). Advanced Encryption Standard Using FPGA Overnetwork. *EUREKA, Physics and Engineering*, 1, 32–39.

Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues. *Journal of Network and Computer Applications*, 98, 27–42.

Huda, S. M. A., & Moh, S. (2022). Survey on Computation Offloading in UAV-Enabled Mobile Edge Computing. *Journal of Network and Computer Applications*, 201(2), 1-26.

Hudson, H. E., Forsythe, V., & Burns, S. G. (1983). Keeping in Touch by Two-Way Radio. *World Health Forum*, *4*(2), 157–161.

Ibrahim, M. H. (2016). Octopus: An Edge-Fog Mutual Authentication Scheme. *International Journal of Network Security*, 18(6), 1089–1101.

Indrasena Reddy, M., Siva Kumar, A. P., & Subba Reddy, K. (2020). A Secured Cryptographic System Based on DNA and a Hybrid Key Generation Approach. *BioSystems*, 197, 1-10.

Jain, S., & Bhatnagar, V. (2014). Analogy of various DNA based security algorithms using cryptography and steganography. *In 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 285-291.

Jiang, C., Zhang, Y., Wang, F., & Liu, H. (2021). Toward Smart Information Processing with Synthetic DNA Molecules. *Macromolecular Rapid Communications*, 42(11), 1–17.

Jimoh, Y., and Abdulhamid, Shafi' (2018). Dragonfly Algorithm based Detection Technique for Man-In-The-Middle Attack in Fog Computing Environment. *Proceedings of the 1st National Communication Engineering Conference*, 1-6.

Jung, C. J., Menoret, S., Brusselle, L., Tesson, L., Usal, C., Chenouard, V., Remy, S., Ouisse, L. H., Poirier, N., Vanhove, B., De Jong, P. J., & Anegon, I. (2016). Comparative Analysis of PiggyBac, CRISPR/Cas9 and TALEN Mediated BAC Transgenesis in the Zygote for the Generation of Humanized SIRPA Rats. *Scientific Reports*, 6(7), 1–13.

Kaedi, S., Doostari, M. A., & Ghaznavi-Ghoushchi, M. B. (2018). Low-Complexity and Differential Power Analysis (DPA)-Resistant Two-Folded Poweraware

Rivest-Shamir-Adleman (RSA) security schema implementation for IoT-connected devices. *IET Computers and Digital Techniques*, 12(6), 279–288.

Kalaria, R., Kayes, A. S. M., Rahayu, W., & Pardede, E. (2021). A Secure Mutual Authentication Approach to Fog Computing Environment. *Computers and Security*, 111, 1-13.

Kalsi, S., Kaur, H., & Chang, V. (2018). DNA Cryptography and Deep Learning Using Genetic Algorithm with NW algorithm for Key Generation. *Journal of Medical Systems*, 42(1), 1-12.

Karthick, R., Ramkumar, R., Akram, M., & Kumar, M. V. (2021). Overcome the Challenges in Bio-medical Instruments Using IoT - A Review. *Materials Today: Proceedings*, 45, 1614–1619.

Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography. *Introduction to Modern Cryptography*, 1–527.

Kaur, U., & Singh, D. (2014). A Survey on Summarizers and its Applications. *International Journal of Current Engineering and Technology*, *4*(1), 80–83.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82, 395-411.

Khan, S., Parkinson, S., & Qin, Y. (2017). Fog Computing Security: A Review of Current Applications and Security Solutions. *Journal of Cloud Computing*, 6*(*1), 1-22.

Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I., & Ahmed, A. (2019). Edge Computing: A Survey. *Future Generation Computer Systems*, *97*, 219–235.

Khanagha, S., Ansari, S., Paroutis, S., & Oviedo, L. (2022). Mutualism and the Dynamics of New Platform Creation: A Study of Cisco and Fog Computing. *Strategic Management Journal*, 43(3), 476–506.

Kim, S. H., & Lee, I. Y. (2018). IoT Device Security Based on Proxy Re-Encryption. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 1267–1273.

Koblitz, B. N. (1987). Elliptic Curve Cryptosystems. 4(177), 203–209.

Koo, D., & Hur, J. (2018). Privacy-Preserving Deduplication of Encrypted Data with Dynamic Ownership Management in Fog Computing. *Future Generation Computer Systems*, 78, 739–752.

Kordov, K. M. (2014). Modified Chebyshev Map Based Pseudo-random bit Generator.

In AIP Conference Proceedings, 432-436.

Kraemer, F. A., Braten, A. E., Tamkittikhun, N., & Palma, D. (2017). Fog Computing in Healthcare-A Review and Discussion. *IEEE Access*, 5, 9206–9222.

Kumaraguru, P. V., & Chakravarthy, V. J. (2018). DNA Based Cryptography Using Encryption Scheme for Data Security. *Asian J Appl Res*, 4(3) 1-10.

Lee, K., Kim, D., Ha, D., Rajput, U., & Oh, H. (2015). On Security and Privacy Issues of Fog Computing Supported Internet of Things Environment. *In 2015 6th International Conference on the Network of the* Future (NOF), 1-3.

Li, C., Qin, Z., Novak, E., & Li, Q. (2017). Securing SDN Infrastructure of IoT-Fog Networks from MitM Attacks. *IEEE Internet of Things Journal*, 4(5), 1156–1164.

Lin, H. Y., Tsai, T. T., Ting, P. Y., & Chen, C. C. (2022). An Improved ID-Based Data Storage Scheme for Fog-Enabled IoT Environments. *Sensors*, 22(11), 4223.

Liu, B. (2018). BioSeq-Analysis: A Platform for DNA, RNA and Protein Sequence Analysis Based on Machine Learning Approaches. *Briefings in Bioinformatics*, 20(4), 1280–1294.

Liu, G., Wu, J., & Wang, T. (2021). Blockchain-Enabled Fog Resource Access and Granting. *Intelligent and Converged Networks*, *2*(2), 108–114.

Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT. *IEEE Access*, 5(X), 3302–3312.

Luan, T. H., Gao, L., Li, Z., Xiang, Y., Wei, G., & Sun, L. (2015). Fog Computing: Focusing on Mobile Users at the Edge. *arXiv preprint arXiv:*1502–1510.

Lucca, A. V., Sborz, G. A. M., Leithardt, V. R. Q., Beko, M., Zeferino, C. A., & Parreira, W. D. (2021). A Review of Techniques for Implementing Elliptic Curve Point Multiplication on Hardware. *Journal of Sensor and Actuator Networks*, 10(1), 1-10.

Lutz, Mark. *Programming python*. " O'Reilly Media, Inc.", 2001.

Lyu, L., Jin, J., Rajasegarar, S., He, X., & Palaniswami, M. (2017). Fog-Empowered Anomaly Detection in IoT Using Hyperellipsoidal Clustering. *IEEE Internet of Things Journal*, 4(5), 1174–1184.

Mahto, D., & Kumar Yadav, D. (2018). Performance Analysis of RSA and Elliptic

Curve Cryptography. *International Journal of Network Security*, 20(4), 625–635.

Mahto, D., & Yadav, D. K. (2017). RSA and ECC: A Comparative Analysis. *International Journal of Applied Engineering Research*, 12(19), 9053–9061.

Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors*, *22*(6), 2087.

Malhotra, M., & . G. (2019). DNA Cryptography (2019): A Novel Approach for Data Security Using Flower Pollination Algorithm. *SSRN Electronic Journal*, 2069–2076.

Malik, U. M., Javed, M. A., Zeadally, S., & Islam, S. ul. (2021). Energy Efficient Fog Computing for 6G Enabled Massive IoT: Recent trends and future opportunities. *IEEE Internet of Things Journal*, 46(c), 1–22.

Mann, Z. Á. (2021). Notions of Architecture in Fog Computing. *Computing*, *103*(1), 51–73.

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A Survey on Mobile Edge Computing: The Communication Perspective. *ArXiv*, 19(4), 2322–2358.

Martin, B. A., Michaud, F., Banks, D., Mosenia, A., Zolfonoon, R., Irwan, S., & Zao, J. K. (2017). Openfog Security Requirements and Approaches. *In 2017 IEEE Fog World Congress (FWC)*, 1-6.

Marton, K., & Suciu, A. (2015). On the interpretation of results from the NIST statistical test suite. *Science and Technology*, 18(1), 18-32.

Mitsophonsiri, K., Punthawanunt, S., Mitatha, S., & Yupapin, P. P. (2011). Data Security Transmission via a Noisy Channel. *Procedia Engineering*, 8, 487-492.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, 36(1), 42–57.

Mohammed Sadeeq, M., Abdulkareem, N. M., Zeebaree, S. R. M., Mikaeel Ahmed, D., Saifullah Sami, A., & Zebari, R. R. (2021). IoT and Cloud Computing Issues, Challenges and Opportunities: A Review. *Qubahan Academic Journal*, 1(2), 1–7.

Mohammed, M. A., Abood, L. K., & Maliki, M. (2017). Mathematical Message Authentication Code Using S-Box key. *IJCSNS*, 17(7), 31-37.

Mohan, N., & Kangasharju, J. (2016). Edge-Fog cloud: A Distributed Cloud for Internet of Things Computations. *In 2016 Cloudification of the Internet of Things (CIoT)*, 1-6.

Mollah, M. B., Azad, A. K., & Vasilakos, A. (2017). Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things. *IEEE Cloud Computing*, 4(1), 34–42.

Mondal, Mandrita, and Kumar S. Ray (2019). Review on DNA cryptography. *arXiv preprint arXiv*:1904-1908.

Mukherjee, B., Neupane, R. L., & Calyam, P. (2017). End-to-End IoT Security Middleware for Cloud-Fog Communication. *In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 151-156.

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and Privacy in Fog Computing: Challenges. *IEEE Access*, 5, 19293-19304.

Munir, A., Kansakar, P., & Khan, S. U. (2017). IFCIoT: Integrated Fog Cloud IoT. *IEEE Consumer Electronics Magazine*, *6*(3), 74–82.

Munir, N., Khan, M., Shah, T., Alanazi, A. S., & Hussain, I. (2021). Cryptanalysis of Nonlinear Confusion Component Based Encryption Algorithm. *Integration*, *79*(January), 41–47.

Namasudra, S. (2020). Fast and Secure Data Accessing by using DNA Computing for the Cloud Environment. *IEEE Transactions on Services Computing*, 1374(c), 1–12.

Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing Multimedia by using DNA-based Encryption in the Cloud Computing Environment. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),16*(3s), 1–19.

Namasudra, S., Sharma, S., Deka, G. C., & Lorenz, P. (2020). DNA Computing and Table Based Data Accessing in the Cloud Environment. *Journal of Network and Computer Applications*, *172*, 1–13.

Nath, S. B., Gupta, H., Chakraborty, S., & Ghosh, S. K. (2018). A Survey of Fog

Computing and Communication: Current Researches and Future Directions. *arXiv preprint arXiv:*1804–1809.

Nguyen, V; Lin, P; Hwang, R. (2018). Distributed DoS Defense Architecture for Mobile Networks. *IEEE Network*, 32(1), 118–124.

Ni, J., Zhang, K., Lin, X., & Shen, X. S. (2018). Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. *IEEE Communications Surveys and Tutorials*, 20(1), 601–628.

Nourildean, S. W., Hassib, M. D., & Mohammed, Y. A. (2022). Internet of things based wireless sensor network: a review. *Indones. J. Electr. Eng. Comput. Sci*, *27*(1), 246-261.

Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors*, 22(3), 1–27.

Osanaiye, O., Chen, S., Yan, Z., Lu, R., Choo, K. K. R., & Dlodlo, M. (2017). From cloud to fog computing: A Review and a Conceptual live VM Migration Framework, *IEEE Access*, 5, 8284-8300.

Pallewatta, S., Kostakos, V., & Buyya, R. (2022). QoS-Aware Placement of Microservices-Based IoT Applications in Fog computing Environments. *Future Generation Computer Systems*, 131, 121–136.

Pamarthi, S., & Narmadha, R. (2022). Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, *10*(4), 482-506.

Pan, J., & McElhannon, J. (2018). Future Edge Cloud and Edge Computing for Internet of Things Applications. *IEEE Internet of Things Journal*, 5(1), 439–449.

Park, B., Song, J., & Seo, S. C. (2020). Efficient Implementation of a Crypto Library Using Web Assembly. *Electronics (Switzerland)*, 9(11), 1–23.

Parveen, K., Zaidi, N., & Choudhury, T. (2016). Fog Computing: Common Security Issues and Proposed Countermeasures. *In 2016 International Conference System Modeling & Advancement in Research Trends (SMART*), 311-315.

Pattewar, G., Mahamuni, N., Nikam, H., Loka, O., & Patil, R. (2022). Management of IoT devices security using blockchain—a review. *Sentimental Analysis and Deep Learning: Proceedings of ICSADL*, 735-743.

Pavithran, P., Mathew, S., Namasudra, S., & Lorenz, P. (2021). A Novel Cryptosystem Based on DNA Cryptography and Randomly Generated Mealy Machine. *Computers & Security*, 104, 1-13.

Popentiu-Vladicescu, F., & Albeanu, G. (2017, April). Software Reliability in the Fog Computing. *In 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)*, 1-4.

Pourkiani, M., & Abedi, M. (2019). An Introduction to a Dynamic Data Size Reduction Approach in Fog Servers. *2019 International Conference on Information and Communications Technology, ICOIACT* , 261–265.

Preetha, D. M. (2019). Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing. *International Journal for Research in Applied Science and Engineering Technology*, 7(3), 1145–1147.

Puthal, D., Mohanty, S. P., Bhavake, S. A., Morgan, G., & Ranjan, R. (2019). Fog Computing Security Challenges and Future Directions Energy and Security. *IEEE Consumer Electronics Magazine*, 8(3), 92–96.

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). Threats to Networking Cloud and Edge Datacenters in the Internet of Things. *IEEE Cloud Computing*, *3*(3), 64–71.

Rahman, A., Uddin, M., Riaz, H., Nath, N., & Pathan, A. Q. M. S. (2019). A Fog Based Encryption Algorithm for IoT Network. *International Journal of Computer Science and Information Security (IJCSIS)*, 17(4), 199–204.

Raj, B. B., & Sharmila, V. C. (2018). An Survey on DNA Based Cryptography. *In 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)*,1-3.

Rani, R., Kumar, N., Khurana, M., Kumar, A., & Barnawi, A. (2021). Storage as a Service in Fog computing: A systematic Review. *Journal of Systems Architecture*, 116, 1-13.

Rath, M., & Rout, U. P. (2015). Analysis and Study of Security Aspect and Application Related Issues at the junction of MANET and IoT. International Journal of Research in Engineering and Technology, 4(13), 426-430.

Rios, R., Roman, R., Onieva, J. A., & Lopez, J. (2017). From SMOG to Fog: A Security Perspective. *2017 2nd International Conference on Fog and Mobile*

Edge Computing, 56–61.

Rogers, I., Harrell, G., & Wang, J. (2013). Using π digits to Generate Random Numbers : A Visual and Statistical Analysis. *International Conference on Scientific Computing*, 251–257.

Roig, P. J., Alcaraz, S., Gilly, K., Bernad, C., & Juiz, C. (2021). Modeling of a Generic Edge Computing Application Design. *Sensors*, *21*(21), 1-29.

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile Edge Computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78, 680–698.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., & Vo, S. (2001). *NIST Special Publication 800-22 (with revisions dated. 22)*, 1-140.

Sabireen, H., & Neelanarayanan, V. (2021). A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ICT Express*, 7(2), 162–176.

Sadhukhan, D., Ray, S., Biswas, G. P., Khan, M. K., & Dasgupta, M. (2021). A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, 77, 1114-1151.

Sahmim, S., & Gharsellaoui, H. (2017). Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. *Procedia computer science*, 112, 1516-1522.

Sahni, Y., Cao, J., Zhang, S., & Yang, L. (2017). Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things. *IEEE Access*, 5(c), 16441–16458.

Sareen, P. (2016). The Fog Computing Paradigm. *International Journal of Emerging Technologies in Engineering Research*, 4(8), 55–60.

Sarkar, S., Chatterjee, S., & Misra, S. (2015). Assessment of the Suitability of Fog Computing in the Context of Internet of Things. *IEEE Transactions on Cloud Computing*, 6(1), 46-59.

Satir, E., & Kendirli, O. (2022). A symmetric DNA Encryption Process with a Biotechnical Hardware. *Journal of King Saud University-Science*, 34(3), 1-13.

Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2022). Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. Cluster Computing, 25(3), 1729-1748.

Shah, R., & Pippal, R. S. (2021). Cloud Data Storage Security by Applying Modified DNA Cryptography. *Research Journal of Engineering Technology and Medical Sciences*, 4(3), 29-35.

Shahzad, M., & Singh, M. P. (2017). Continuous Authentication and Authorization for the internet of things. *IEEE Internet Computing*, 21(2), 86–90.

Shakarami, A., Shakarami, H., Ghobaei-Arani, M., Nikougoftar, E., & Faraji-Mehmandar, M. (2022). Resource Provisioning in Edge/Fog Computing: A Comprehensive and Systematic Review. *Journal of Systems Architecture*, 122, 1-13.

Sharma, S., & Verma, V. K. (2022). An integrated exploration on internet of things and wireless sensor networks. *Wireless Personal Communications*, *124*(3), 2735-2770

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, *3*(5), 637–646.

Shi, Y., Ding, G., Wang, H., Roman, H. E., & Lu, S. (2015). The Fog Computing Service for healthcare. In 2015 2nd *International Symposium on FutureInformation and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech)*, 1-5.

Shiny, S. J. (2022). A Review on Application of MANET-IoT. i-manager's *Journal on Mobile Applications and Technologies*, 9(1), 28.

Sierra, J. M., Hernández, J. C., Alcaide, A., & Torres, J. (2004). Validating the Use of BAN LOGIC. *In International Conference on Computational Science and Its Applications*, 851-858.

Silva, R., Silva, J. S., & Boavida, F. (2017). Opportunistic Fog Computing: Feasibility Assessment and Architectural Proposal. *In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 510-516. IEEE.

Singh, C., Chauhan, D., Deshmukh, S. A., Vishnu, S. S., & Walia, R. (2021). Medi-Block record: Secure data sharing using block chain technology. Informatics in Medicine Unlocked, 24, 100624.

Singh, S. P., Nayyar, A., Kumar, R., & Sharma, A. (2019). Fog Computing: from

Architecture to Edge Somputing and big data processing. *The Journal of Supercomputing,* 75(4), 2070-2105.

Singh, Shivendra, Sarfaraz Iqbal, M., & Jaiswal, A. (2015). Survey on Techniques Developed using Digital Signature: Public Key Cryptography. *International Journal of Computer Applications*, 117(16), 1–4.

Singh, Sunakshi, & Chaurasiya, V. K. (2021). Mutual Authentication Scheme of IoT Devices in Fog Computing Environment. *Cluster Computing*, *24*(3), 1643–1657.

Sitton-Candanedo, I., Alonso, R. S., Corchado, J. M., Rodriguez-Gonzalez, S., & Casado-Vara, R. (2019). A Review of Edge Computing Reference Architectures and a new Global Edge Proposal. *Future Generation Computer Systems*, 99, 278–294.

Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers and Security*, *74*, 340–354.

Sreeja, C. S., Misbahuddin, M., & Hashim, N. M. (2014). DNA for Information Security: A Survey on DNA Computing and a Pseudo DNA Method Based on Central Dogma of Molecular Biology. *In International Conference on Computing and Communication Technologies*, 1-6.

Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security issues. *In 2014 federated conference on computer science and information systems*, 1-8.

Stojmenovic, I., Wen, S., Huang, X., & Luan, H. (2016). An Overview of Fog Computing and its Security Issues. *Concurrency and Computation: Practice and Experience*, 28(10), 2991-3005.

Stolfo, S. J., Salem, M. B., & Keromytis, A. D. (2012). Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. *In 2012 IEEE symposium on security and privacy workshops,* 125-128.

Su, H. J., Castro, C. E., Marras, A. E., & Zhou, L. (2017). The Kinematic Principle for Designing Deoxyribose Nucleic Acid Origami Mechanisms: Challenges and Opportunities1. *Journal of Mechanical Design*, *139*(6), 1-9.

Sun, Y., Lin, F., & Zhang, N. (2018). A Security Mechanism Based on Evolutionary

Game in Fog Computing. *Saudi Journal of Biological Sciences*, 25(2), 237–241.

Swessi, D., & Idoudi, H. (2022). A survey on internet-of-things security: threats and emerging countermeasures. *Wireless Personal Communications*, 124(2), 1557-1592.

Thabit, F., Alhomdy, S., & Jagtap, S. (2021). A New Data Security Algorithm for the Cloud Computing Based on Genetics Techniques And Logical-Mathematical Functions. *International Journal of Intelligent Networks*, 2, 18-33.

Thiruthuvadoss, A. P. (2012). Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography. A M. Sc. Dissertation, Dept. of System on Chip Design, Royal Institute of Technology.

Tornea, O., Borda, M. E., & Pileczki, V. (2018). Cryptographic Algorithm Based on Dna and RNA Properties. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 7(11), 237–241.

Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M., & Cerny, T. (2022). Systematic review of authentication and authorization advancements for the Internet of Things. *Sensors*, 22(4), 1361.

UbaidurRahman, N. H., Balamurugan, C., & Mariappan, R. (2015). A Novel DNA Computing Based Encryption and Decryption Algorithm. *Procedia Computer Science*, 46, 463-475.

Varghese, B., Wang, N., Barbhuiya, S., Kilpatrick, P., & Nikolopoulos, D. S. (2016). Challenges and Opportunities in Edge Computing. *In 2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 20-26.

Varshney, P., & Simmhan, Y. (2017). Demystifying Fog Computing: Characterizing Architectures, Applications and Abstractions. *In 2017 IEEE 1st international conference on fog and edge computing (ICFEC)*, 115-124.

Venkataraman, K., & Sadasivam, T. (2019). FPQA implementation of modified Elliptic Curve Digital Signature Algorithm. *Facta Universitatis - Series: Electronics and Energetics*, 32(1), 129–145.

Venu, D., Arun Kumar, A., & Vaigandla, K. K. (2022). Review of Internet of Things (IoT) for Future Generation Wireless Communications. *International Journal for Modern Trends in Science and Technology*, 8(03), 01-08.

Verma, M., Bhardwaj, N., & Yadav, A. K. (2016). Real Time Efficient Scheduling Algorithm for Load Balancing in Fog Computing Environment. *International Journal of Information Technology and Computer Science*, 8(4), 1–10.

Vijaykumar, J., Rajkumar, P., & Kandan, S. R. (2021). Fog Computing Based Secured Mobile Cloud for Cumulative Integrity in Smart Environment and Internet of Things. *Materials Today: Proceedings*, 8(9),2221-2236.

Wadday, A. G., Wadi, S. M., Mohammed, H. J., & Abdullah, A. A. (2018). Study of WiMAX Based Communication Channel Effects on the Ciphered Image Using MAES Algorithm. *International Journal of Applied Engineering Research*, 13(8), 6009–6018.

Wang, L., An, H., & Chang, Z. (2020). Security enhancement on a lightweight authentication scheme with anonymity fog computing architecture. *IEEE Access*, 8, 97267-97278.

Wang, Q., Chen, D., Zhang, N., Ding, Z., & Qin, Z. (2017). PCP: A Privacy-Preserving Content-Based Publish-Subscribe Scheme with Differential Privacy in Fog Computing. *IEEE Access*, 5, 17962–17974.

Wang, X., Yang, L. T., Xie, X., Jin, J., & Deen, M. J. (2017). A Cloud-Edge Computing Framework for Cyber-Physical-Social Services. *IEEE Communications Magazine*, 55(11), 80-85.

Wang, Y., Uehara, T., & Sasaki, R. (2015). Fog computing: Issues and Challenges in Security and Forensics. *In 2015 IEEE 39th annual computer software and applications conference*, 53-59.

Watson, F. C., Wilkins, M., Center, R. F., & Image, B. (2007). The Structure of DNA: Cooperation and Competition.

Wen, Z., Yang, R., Garraghan, P., Lin, T., Xu, J., & Rovatsos, M. (2017). Fog orchestration for internet of things services. *IEEE Internet Computing*, *21*(2), 16–24.

Yi, S., Li, C., & Li, Q. (2015). A survey of Fog Computing: Concepts, Applications and Issues. *In Proceedings of the 2015 workshop on mobile big data*, 37-42.

Yousefpour, A., Ishigaki, G., & Jue, J. P. (2017). Fog computing: Towards Minimizing Delay in the Internet of Things. *In 2017 IEEE international conference on edge computing (EDGE)*, 17-24.

Yusof, A. R. A., Udzir, N. I., & Selamat, A. (2019). Systematic Literature Review and Taxonomy for DDoS Attack Detection and Prediction. *International Journal of Digital Enterprise Technology*, 1(3), 292-315.

Zhang, P., Chen, Z., Liu, J. K., Liang, K., & Liu, H. (2018). An efficient Access Control Scheme with Outsourcing Capability and Attribute Update for Fog Computing. *Future Generation Computer Systems*, 78, 753–762.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud Computing: State-of-the-art and Research Challenges. *Journal of Internet Services and Applications*, 1(1), 7–18.

Zhang, X., Zhou, Z., & Niu, Y. (2018). An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding. *IEEE Photonics Journal*, *10*(4), 1–14.

Zhang, Y., Wang, Z., Wang, Z., Karanfil, Y. H., & Dai, W. (2016). A new DNA Cryptography Algorithm Based on the Biological Puzzle and DNA chip Techniques. *In International Conference on Biomedical and Biological Engineering*, 360-365.

Zhang, Yuexin, Xiang, Y., Wu, W., & Alelaiwi, A. (2018). A Variant of Password Authenticated Key Exchange Protocol. *Future Generation Computer Systems*, *78*, 699–711.

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, 55(1), 26-33.

VITA

The author was born on February 25, 1989, in Dir Lower, Khyber Pakhtunkhwa, Pakistan. He was educated for his primary education from 1995 to 1999 and high school from 2000 to 2004 in Dir Lower, Maidan,Khyber Pakhtunkhwa, Pakistan respectively. He furthered studied his F.SC (Pre-Eng) education in Dir Lower, Chakdara, Khyber Pakhtunkhwa, Pakistan from 2005 to 2006. After that, he then pursued his bachelor study at the University of Malakand in 2007 and graduated in December 2011. He entered The University of Agriculture Peshawar Pakistan in 2012 and completed his Masters in Computer Science (MSCS) in August 2015. He was a lecturer in Computer Science at Global Degree College Peshawar Pakistan from 2012 to September 2017. He is currently pursuing his studies in the philosophy of Information Technology at Universiti Tun Hussein Onn Malaysia, Johor, Malaysia. His research interests are cryptography, DNA Cryptography, Authentication, key exchange protocols, and Man in the Middle attack.