International Journal of Modern Computation, Information, and Communication Technology
2023;6(2):59-64.
ISSN: 2581-5954

Network Security with Cryptography

J. Umamageswaran[1*], B. Praveen Kumar[1], R. Dhanalakshmi[1], A.V. Kalpana[1]

[1]*Department of Information Technology, R.M.K Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India.*
[2]*Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India.*
[3]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India.*
[4]*Department of Artificial Intelligence, Shri Vishnu Engineering College for Women, Bhimavaram, Andra Pradesh, India.*

[*]*Corresponding author: j.umamageswaran@gmail.com*

Abstract. With the proliferation of e-commerce platforms and social media sites, businesses across the globe now produce massive amounts of data daily. Safe data transmission via the Internet relies on several factors, but information security is the most fundamental of them. As society continues its transition into the digital information era, network security challenges are also rising to the forefront. The growing number of people using the Internet makes it a prime target for malicious hackers. Computer and network security, i.e., the crucial challenges, need its implementation. These harmful nodes are a systemic problem. It may make use of other nodes' resources while keeping its own secure. This article presents a high-level introduction to Network Security and the many cryptographic approaches that may be used to strengthen Network Security.

Keywords: Network Security, Cryptography, Cyber-attacks, Information security, Internet

INTRODUCTION

In developing areas, quantum computing exploits quantum mechanical principles to surpass traditional computers. Many aspects of 5G and beyond networks may benefit from quantum computing. Its exponential data processing speed offers solutions to pressing problems in many industries and fields of study. This article presents an in-depth overview of the area, covering everything from the most pressing uses for quantum computers to their potential impact on the future of cryptography. Unstructured search, quantum simulation, and optimization are three of quantum computing's most promising use cases. It also has the potential to boost the efficiency and precision of other technologies, such as machine learning [1]. There are many uses for these innovations in 5G and future networks. Quantum computers have impressive capabilities, but they also present a significant threat to many current security methods, notably asymmetric key cryptography. Mobile broadband standards have shifted away from symmetric keys encryption methods toward a PKI-based trust model in part due to the threat posed by quantum computers. Alternative cryptosystems based on mathematical issues that are thought to be impossible for even quantum computers to solve are also discussed at length. Also, talk about recent progress in quantum key distribution, which uses quantum phenomena to create cryptosystems that are immune to the effects of quantum computing. Such quantum-resistant technologies hold much promise for ensuring the safety of 5G and future networks [2].

Designing a privacy protection system that ensures the secure sharing of UAV big data is essential for finding a workable solution to the issue of privacy protection of UAV large data collected by unmanned aerial vehicles (UAVs). Blockchain technology is used here to address the issue of privacy with big UAV data. Blockchain data is encrypted using a cryptosystem developed by several theory research teams in the suggested privacy protection plan. An examination of privacy is offered to verify the safety measures. Using blockchain technology, the suggested privacy protection strategy for large UAV data offers cheap processing costs for key generation, encryption, and decryption, as shown by the assessment results [3]. It also performs better than the standard methods. The purpose of this paper is to serve as a starting point for further studies on UAV data privacy security. Anti-counterfeiting, information display, and information protection may all benefit from the use of materials with shape-morphing and/or fluorescence imaging capabilities. These features are difficult to implement in hydrogels

Received: 26.08.2023 Revised: 16.10.2023 Accepted: 04.11.2023
Licensed under a CC-BY 4.0 license | Copyright (c) by the authors

because of their subpar mechanical characteristics and fixed fluorescence. This work describes a robust hydrogel with excellent shapes-memory abilities and photos adjustable fluorescence, which enable programmable shape designing and information encodings for dual-encryptions [4]. Dense intra- and inter-chain hydrogen bonds give this hydrogel its desirable properties, such as its higher stiffness, higher toughness, temperatures-mediated shapes-memory properties, and it is prepared by incorporating donors-acceptors chromophore unit into a poly (1-vinylimidazole-co-methacrylic acids) network. The photo-mediated tuning of the hydrogel's fluorescence is due to a chromophore under-to-dimer transition. Hydrogel sheets encoded with fluorescent patterns may be folded into predetermined 3D forms using a combination of photolithography and origami/kirigami designs [5].

Only after sequentially restoring the hydrogels' original shape and exposing them to UV light is it possible to decipher the fluorescent data included in the architectural designs. Proof-of-concept investigations show that both the luminous pattern and the 3D arrangement may be reprogrammed, allowing for the secure storage and re-display of information. Future research on smart materials with enhanced security and broader uses in aquatic conditions should be guided by the creation of robust hydrogels with rewritable luminous patterns and programmable forms [6]. There are many indisputable advantages to using Mobile Cloud Computing (MCC) in health care already, but its expansion is being stymied by concerns about patient privacies and security. Such concerns require immediate attention to reach their full potential and effective use. There is a pressing need to protect sensitive healthcare data on a global, regional, and local scale. Implementing the necessary security procedures for protection against security breaches and vulnerabilities is essential for maximizing the benefits of health services [7]. Based on a tiered concept of security, this study contemplates how to best use the Modular Encryptions Standards (MES) to protect sensitive healthcare information. Based on the results of the performance study, the suggested work provides superior performance and supplementary qualitative security-assuring measures compared to another regularly used algorithm against health information securities in the MCC context.

LITERATURE SURVEY

The distributed ledger technology known as "block chain" is a novel approach to solving the problems of data storage, transaction execution, security, and trust in a decentralized setting. With applications ranging from smart grids and smart contracts to the Internet of Things and beyond, block chains are a technical advancement for cyber security and cryptographies. With the advent of the Internet of Things, there has been a dramatic rise in the need to store and share information through a central server. To enhance securities and privacies in a private block chain, it has been proposed here to use the Internet of Things (IoT) to implement a mechanism called Splitting of proxy re-encryption (Split-PRE). To address trust and scalability issues while also streamlining transactions, this research suggests a blockchain-based proxy re-encryptions mechanism [8]. The encrypted data from the Internet of Things is then stored in a decentralized cloud. Without the need for a reliable third party, the framework allows for the sharing of collected IoT data through dynamics and smart contracts between the sensors and the device users. The data is encrypted using a proxy re-encryptions scheme that only the owners and the smart contract participants know about. The experimental results demonstrate that the suggested technique improves the system's efficiency, security, privacy, and practicality in comparison to the states-of-the-arts [9].

Power shortages, inadequate computational power, poor communication abilities, and susceptibility to assault are only some of the issues plaguing wireless sensor networks (WSN). However, when applied to WSN, the present encryption algorithms cannot efficiently resolve the issues. To this purpose, enhanced identity-based encryption algorithms (IIBE) are presented that may efficiently streamline the key generations processes, lessen the load on the network, and tighten up security in a wireless sensor network (WSN). This algorithm's design philosophy is intermediate between that of classic public key encryptions and that of identity-based public tweezers' encryptions. The approach sidesteps the hassle of managing certificates by not requiring one, unlike conventional methods of public key encryptions. The technique solves the issues of key escrows and key revocations, which plague identity-based public key encryption. Experimental findings from a real-world network reveal IIBE's low power consumption and good security, making it an ideal candidate for use in WSNs where privacy and data integrity are of the utmost importance [10].

As a result of limited satellite power and processing capacity, storage and security are also at a premium in satellite communication systems. There is a high risk of hacking and external interference on satellite communication channels. Security for satellite networks against unauthorized data access and usage is notoriously difficult. This study builds a framework for securing and authenticating communication networks that makes use of both satellite and ground-based infrastructure. The suggested approach uses a multi-step process for achieving

the goals of secure communication, information exchange, registration, and authentication. The data is sent from the satellite to a ground station with powerful data processing capabilities. Any critical parameters are recorded by the ground station, and any certificates from rogue nodes are erased from the distributed ledger. An asymmetric encryption method is used to transmit the key, further bolstering the security of the data transmission. An invulnerability study is carried out under the same attack circumstances to determine how secure the proposed network design is. The outcomes of the simulation trials demonstrate that the suggested strategies significantly enhance the security and protection of the communication channel [11].

By providing data protection and system and participant authentication, several encryption methods aim to reduce the likelihood of cyber assaults. However, thanks to improved access to computing power, crypt-analytic methods have matured into a competitive force in the field of information security. This research disclosed vulnerabilities in a newly proposed encryption method for IoHT that makes use of a chaotic map [12]. The scheme's security claims are based on novel chaotic maps, modified Mandelbrot sets, and conditional shift algorithms. Cryptographic attacks against the understudy cryptosystem recover the key that is used. Because only one plaintext cipher text pair was available, a chosen-plaintext attack was used to recover the key with little computational effort. The attacks' bare-bones execution times reveal the diffusion-based encryption algorithms' weakness. Recommendations to strengthen the underlying cryptographic algorithm's security are provided [13].

Sharing data has become an increasingly important function of the cloud as the Internet of Things has developed. Despite the widespread interest in this technology, one of its key challenges is the need to ensure the safety of sensitive information since any breach of this kind may result in costly consequences. This piece advocates for a proxy re-encryption strategy for safe cloud-based information exchange. Using identity-based encryption, data owners may send encrypted files to the cloud, where they'll be accessible only to authorized users thanks to proxy re-encryption. Due to their limited resources, IoT gadgets rely on a proxy server located at the network's periphery, or "edge," to do data-demanding calculations [14]. In addition, takes advantage of the characteristics of information-centric networking to efficiently provide proxy-cached material, which boosts service quality and makes efficient use of available network resources. Our system's blueprint is founded on blockchain, a game-changing innovation that makes distributed data sharing possible. It helps alleviate the inefficiencies of a centralized system and allows for granular control over data access. Our strategy shows promise in protecting the privacy and integrities of sensitive information, as shown by the results of our security investigation and review [15].

PROPOSED SYSTEM

The term "security" is quite all-encompassing. In its most basic form, it is concerned with preventing eavesdroppers from reading or, worse, surreptitiously altering communications meant for other receivers. Its focus is on preventing unauthorized access to distant services. Most security issues are triggered deliberately by people who want to exploit the situation for their own ends. Issues with network security may be broken down into approximately four interconnected categories: a) Confidentiality; b) Authenticity; c) non-repudiation; d) Controlled Integrity. Confidentiality, sometimes known as secrecy, refers to the practice of shielding sensitive information from prying eyes. Authentication is the process of verifying the identities of a person before sharing private information or concluding a transaction. In the context of any application-to-applications communications, no repudiation requires authentication, among other security measures. Confidentiality means that no one other than the intended recipient has access to communication. The concept of message integrity refers to the act of guaranteeing to the recipient that the messages they have received are identical to the ones sent. Non-repudiation ensures the original sender cannot deny sending the communication. Name-based and address-based authentication are now the most used methods of host-to-host authentication on the Internet. However, they are both very insecure. The sender and the recipient both need to verify the other's identification to ensure that the other is who or what they claim to be in the message. Human-to-human interaction, with its inherent visual recognition, makes this a simple challenge to tackle. It's not so easy to authenticate parties when they're exchanging communications across a channel where neither side can "see" the other. As an example, why should you trust an email that claims to have been sent by a friend really was sent by that friend? What would you do if someone called you, pretending to be from your bank, and asked for your account number, secret PIN, and account balances to verify your identity? Let's hope not! Privacy/Confidentiality Protecting the confidentiality of communication by ensuring that no one other than the sender and the recipient can decipher its contents. The overall layout of the system is seen in Figure 1.

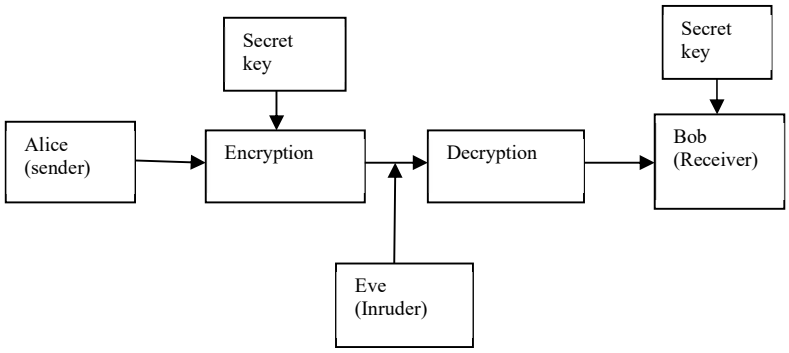

FIGURE 1. System architecture of the proposed system

Communication must be encrypted (data must be disguised) so that it cannot be decoded (understood) by an eavesdropper if it is intercepted. Most people undoubtedly think of this sense of privacy when they hear the phrase "secure communication." However, keeps in mind that this is not just a narrow meaning of encrypted messaging but also a narrow definition of privacy. Consistency of Messages Assuring the recipients that the messages they got are an exact replica of the one sent. Even though the senders and the receivers can verify each other's identity, they still want to make sure the message they transmit to each other doesn't get tampered with. In trustworthy transport and data connection protocols, I came across extensions to the check summing approaches. Refusal to recant the concept of non-repudiation provides a means of verifying the authenticity of a message's originator. Having defined secure communication may go on to defining an "insecure channel." This section focuses on signatures. When an attacker gains access to your system, what data do they have, and what actions may they take? Alice, the sender, wishes to transmit information to Bob, the intended recipient. Alice and Bob will communicate both control messages and data messages (like how TCP senders and receivers share both control segment and data segment) to securely transmit data while fulfilling the criteria of secrecies, authentications, and message integrities. Usually, all or a portion of these communications will be encrypted. Control and data communications on the channel may be monitored and recorded by an active intruder, whereas a passive intruder can just listen to and keep track of them. The term "cryptography" is derived from the Greek, meaning "secret writing."

There is a difference between ciphers and codes, according to experts. A cipher is a method of encoding information by replacing one set of characters with another, bit by bit, regardless of the message's linguistic structure. In contrast, words are swapped out for symbols when using a code. Despite their illustrious past, codes are hardly used nowadays. A function using the key as an input modifies the plaintext or messages to be encrypted. The cipher text, the result of the encryption process, is subsequently sent, often through messenger or radio. The intruder or opponent is assumed to overhear the whole encrypted text and write it down verbatim. However, he is unable to quickly decipher the encrypted text since he is not the intended receiver and hence does not know the decryption key. The intruder may be able to do more than just listen in on the channel (passive intruder), such as actively injecting his own messages or modifying valid ones before they reach the intended recipient. Cryptology refers to both the practice of creating and cracking ciphers. The former is known as cryptanalysis, and the latter as cryptography. Having a notation for relating plaintext, cipher text, and keys can be handy on several occasions. To indicate that cipher text C is the result of applying key K to plaintext P, we will write C = EK (P). Likewise, P = DK(C) stands in for the decryption of C back into plain text.

RESULTS AND DISCUSSIONS

Modern encryption is quite sophisticated. While modern cryptography still has far-reach military implications, it has broadened its domains and is intended to provide a low-cost means of protecting the vast amount of electronic data stored and communicating across corporate networks around the world. Cryptography provides a method for safeguarding this information without compromising the privacy of sensitive financial, medical, or e-commerce details that may otherwise fall into the wrong hands. There have been a lot of breakthroughs in the field of cryptography recently. The Data Encryption Standard (DES) was accepted as a data encryption standard by the National Bureau of Standards (NBS), marking a major step forward in the development of cryptography in the information era. Also, the American National Standards Institute (ANSI) approved the use of the same DES algorithm, which helped bring encryption to the business world. Another important step forward occurred soon after when a novel idea was offered to further Public Key Cryptography (PKC), the development of which is still

ongoing to this day. Both symmetric and asymmetric cryptosystems exist. Symmetric cryptosystems encrypt and decode data or communications using the same secret keys. In contrast, asymmetric cryptosystems encrypt messages or data using one key (the public key) and decode them with a different key (the secret key). This is why public key cryptosystems are another name for asymmetric ones. The absence of a safe mechanism for the people wishing to encrypt their data or conversations to share the secret key has always been a major flaw of symmetric cryptosystems. This issue is addressed by public key cryptosystems, which utilize cryptographic algorithms to generate both the public keys and the secret keys (DES and the much more secure RSA have been considered). Figure 2 depicts the likelihood of delay relative to the likelihood of assault. Number of nodes versus time in milliseconds is shown on Fig. 3.

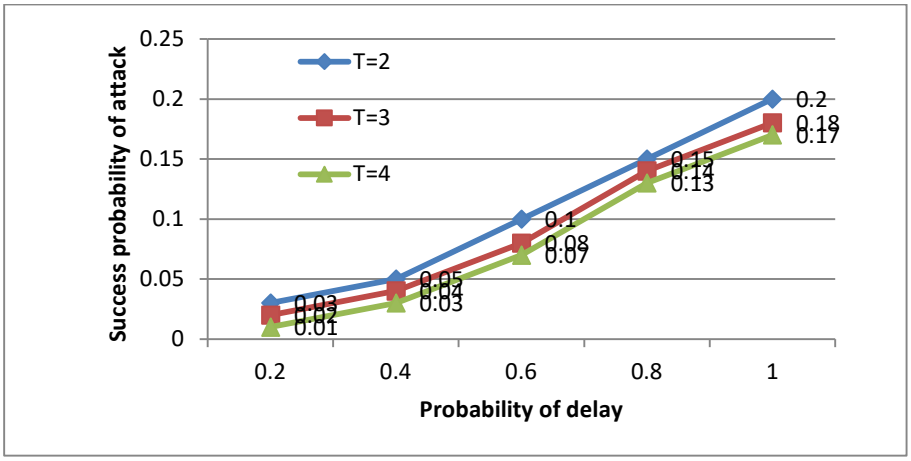

FIGURE 2. Probability of Delay

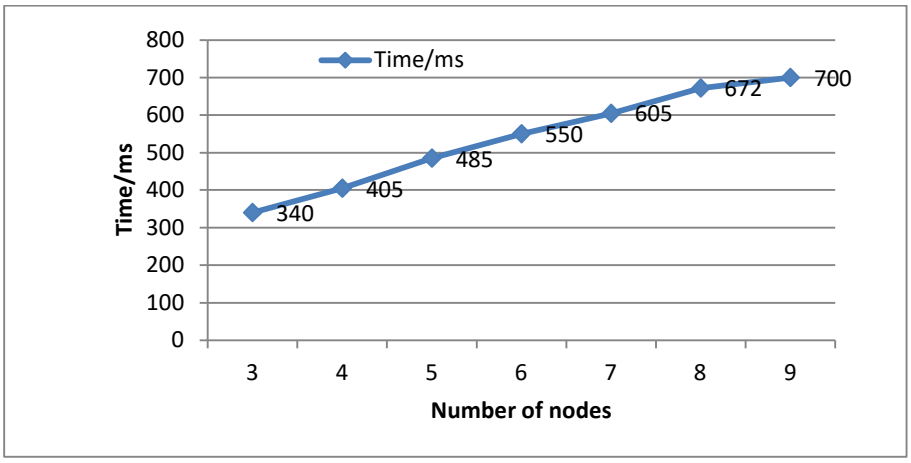

FIGURE 3. Number of nodes with time/ms

Ron Rivests, Adi Shamir, and Leonard Adlemans of the Massachusetts Institute of Technology (MIT) created the RSA algorithm; the most widely used public key cryptosystem. The public key in the RSA algorithm is generated by multiplying two big (100 digits or more) randomly selected prime integers, while the encryption key is generated by selecting a second large number at random. The product of these two primes would then join the encryption key to form the public key. This article provides a high-level overview of cryptography and its operation. Warning: this work does not include cryptanalysis or attacks on cryptosystems. Thus, readers should be aware that there are several methods to break each of these systems. The need for secrecy in the cryptography sector makes for some fascinating research. The irony is that a cryptographic algorithm's security does not depend on its being kept secret. Even if you don't understand the math behind an algorithm, you may trust that it has been well tried and examined if it is widely recognized and published. Any cryptographic method that continues to be

used year after year is likely to be a good one since time is the only genuine test of good cryptography. Key selection (and management) is important to the efficacy of cryptography.

CONCLUSION

Due to the volatile nature of the Internet, system and information security have become a mandatory concern for every organization whose internal private networks use Internet connections. The importance of data encryption has grown throughout the years. Concerns about the safety of sensitive client data have centered on cloud computing. As more sophisticated tools become available, cryptographic frameworks can accommodate a growing number of keys inside a single use case. Several techniques used in cryptography for Network security were presented in this study. A major way to acquire robust security in the cloud is to encode messages using a key known only by the sending and receiving end. The exchanges of keys between the senders and the receiver are crucial tasks. The central administrations persistently classify secret information from unauthorized users. It may also verify the authenticity of the sent message by checking its credibility. Security measures in place may include the implementation of cryptographic computations inside established protocols and software programs. This study provides a concise introduction to the concept of computer security, discusses potential threats to PC system security, and suggests that further research into key circulation and administration, as well as optimum cryptography calculation for data protection over the cloud, is warranted.

REFERENCES

[1]. V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, 2021, "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," *Computer Communications*, **176**, pp. 99-118.

[2]. Z. Lv, L. Qiao, M.S. Hossain, and B.J. Choi, 2021, "Analysis of using blockchain to protect the privacy of drone big data," *IEEE Network*, **35(1)**, pp. 44-49.

[3]. C.N. Zhu, T. Bai, H. Wang, J. Ling, F. Huang, W. Hong, Q. Zheng, and Z. L. Wu, 2021, "Dual-encryption in a shape-memory hydrogel with tunable fluorescence and reconfigurable architecture," *Advanced Materials*, **33(29)**, pp. 1-12.

[4]. M. Shabbir, A. Shabbir, C. Iwendi, A. R. Javed, M. Rizwan, N. Herencsar, and J.C. Lin, 2021, "Enhancing security of health information using modular encryption standard in mobile cloud computing," *IEEE Access*, **9**, pp. 8820-8834.

[5]. B.S. Rawal, G. Manogaran, and M. Hamdi, 2021, "Multi-tier stack of block chain with proxy re-encryption method scheme on the internet of things platform," *ACM Transactions on Internet Technology*, **22(2)**, pp. 1-20.

[6]. C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, 2021, "IIBE: an improved identity-based encryption algorithm for WSN security," *Security and Communication Networks*, **2021**, pp. 1-8.

[7]. C. Li, X. Sun, and Z. Zhang, 2021, "Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology," *IEEE Access*, **9**, pp. 113558-113565.

[8]. N. Munir, M. Khan, M.M. Hazzazi, A. Aljaedi, A.R. Alharbi, and I. Hussain, 2021, "Cryptanalysis of internet of health things encryption scheme based on chaotic maps," *IEEE Access*, **9**, pp. 105678-105685.

[9]. K.O. Agyekum, Q. Xia, E.B. Sifah, C.N. Cobblah, H. Xia, and J. Gao, 2021, "A proxy re-encryption approach to secure data sharing on the internet of things based on blockchain," *IEEE Systems Journal*, **16(1)**, pp. 1685-1696.

[10]. S. Kumar, G. Karnani, M.S. Gaur, and A. Mishra, 2021, "Cloud security using hybrid cryptography algorithms," *2nd International conference on intelligent engineering and Management*, pp. 599-604.

[11]. S. Liu, X. Liu, J. JYuan, and J. Bao, 2021, "Multidimensional information encryption and storage: when the input is light," *Research*," pp. 1-5.

[12]. Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, 2021, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, **23(3)**, pp.1-16.

[13]. H. Fang, and Q. Qian, 2021, "Privacy preserving machine learning with homomorphic encryption and federated learning," *Future Internet*," **13(4)**, pp. 1-20.

[14]. S. Katsikeas, P. Johnson, M. Ekstedt, and R. Lagerström, 2021, "Research communities in cyber security: A comprehensive literature review," *Computer Science Review*, **42**, pp. 1-24.

[15] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, 2021, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach," *IEEE Transactions on Network Science and Engineering*, **9(1)**, pp. 271-281.