[1] **Eman Ibrahim Alyasin**

Oguz Ata[2]

Bilal A. Ozturk[3]

Applied Machine learning İn Beyond the HTTPS With Transport Layer Security (TLS)

Abstract: **-** Today, access to the internet can no longer be considered an additional or luxury since it is a part of our everyday lives — communication, entertainment, banking, shopping, etc. Nevertheless, the transmission of the contents may be unsafe if it involves sending it across the internet without proper measures being taken. This is where secure sockets layer (SSL) and its later version, Transport Layer Security (TLS), fit.To ensure that such communication is safeguarded, the world has today become more exposed to the internet and engages in the exchange of a significant amount of data that is often confidential, including login passwords and financial details. This paper will thus take its focus on current literature from the year 2020-2024 to establish the significance of SSL/TLS in safeguarding data transfer.

Keywords: Web security, cryptography, encryption, decryption, SSL: Secure Sockets Layer, TLS: Transport Layer Security, HTTPS: Hypertext Transfer Protocol Secure.

INTRODUCTION

The internet plays a central role in communication, business, and information in the ever-advancing world. The internet stores so much information, such as login passwords, financial details, messages, and papers, which are normally meant to be confidential. Yet, those vulnerabilities do come with this kind of dependence on the internet. Our privacy and security could be under threat at any given moment due to data leaks, hacks, and internet frauds. The only factor that remains to be done in this terrain to ensure safe movement is to enhance the protection level.

Imagine trying to convey a personal message and then placing that message in a transparent envelope instead of a sealed one. Literally, anyone can read what is written inside! This is what happens in an unencrypted conversation over the internet. However, there are technologies called Secure Sockets Layer and Transport Layer Security which provide the equivalent of an envelope in the online world where the contents, once sent, can only be decrypted by the receiver.

Understanding how these protocols work enables us to be better-informed users. In this part of the article, we will talk about the way SSL/TLS works in ensuring the communication on the internet. The working principles, increase of the user and many more information will show its influence in the internet security. This knowledge allows us to work in digital space safely and effectively, without many concerns about the privacy of information.

LITERATURE REVIEW

In the context of the research, it is examined that SSL/TLS has become more important analyzing the increase of HTTPS which is the communication protocol using SSL/TLS encryption. This tendency is highlighted by Alcaide et al. (2020) who noted the importance of the subject and explained that participants recognised the threats connected with internet security. The physics here is crucial, and it must be understood. In a brief and easy to understand manner, the Mozilla Foundation (2023) explains the SSL/TLS handshake process to ensure that individuals grasp concepts on how data is protected in transfer between the browser and server.

However, SSL/TLS is only one piece of puzzle in the security problem. The article from the National Institute of Standards and Technology (NIST) [1] presents a more extensive perception as it addresses an entire framework

[1 1,2] Department of E.C.E., Institute of Science, Altinbas University, Istanbul, Turkey

[3]Istanbul Aydin University, Faculty of Engineering . Istanbul, Turkey

Email; emanalyasin20@gmail.com . 203720791@ogr.altinbas.edu.tr,

oguz.ata@altinbas.edu.tr

for the protection of information. Although it is not exhaustive to SSL/TLS, it appreciates the importance of encryption in the security measure framework.

As is not restricted to SSL/TLS it conveys awareness of the role of encryption protocols within a more general security paradigm. In general, the security of the known connections is constantly evolving, and it is important to work on new developments in SSL/TLS. The procedural improvements instigated by various authorities are described in GlobalSign's blog article (2021), emphasizing the efforts to enhance the efficiency of such processes. Critically, this involves sound communication since this is fundamental to the success of the adoption process. Imperva's parallel (2024) enables consumers to understand HTTPS, SSL, and TLS while indicating their differences to ensure that consumers are well informed about the basics of the security protocols in the continuation of communication over the internet.

METHODOLOGY

This assessment adopts a qualitative type of analysis based on ideas from literature, articles, reports, and technical documents regarding SSL/TLS protocols. The purpose of the critical evaluation of these materials is to obtain a comprehensive understanding of SSL/TLS and the advantages of using it for protection of messages exchanged through the Internet.

BEYOND THE HTTPS: HOW SSL AND TSL SECURITY

HTTP (Hypertext Transfer Protocol)

HTTP is an abbreviation for Hypertext send Protocol, which is a protocol (or a defined sequence and syntax for displaying information) used to send data across a network. The HTTP protocol is used for the majority of Internet traffic, which include website content and API calls. Two types of HTTP messages exist requests and replies.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is HTTP which includes encryption and verification. The sole difference between the two protocols is that HTTPS employs TLS (SSL) to encrypt and digitally sign standard HTTP requests and answers [Fig.1]. As a result, HTTPS is far more secure than HTTP. A website that utilizes HTTP has the URL http://, but one that uses HTTPS has https://.

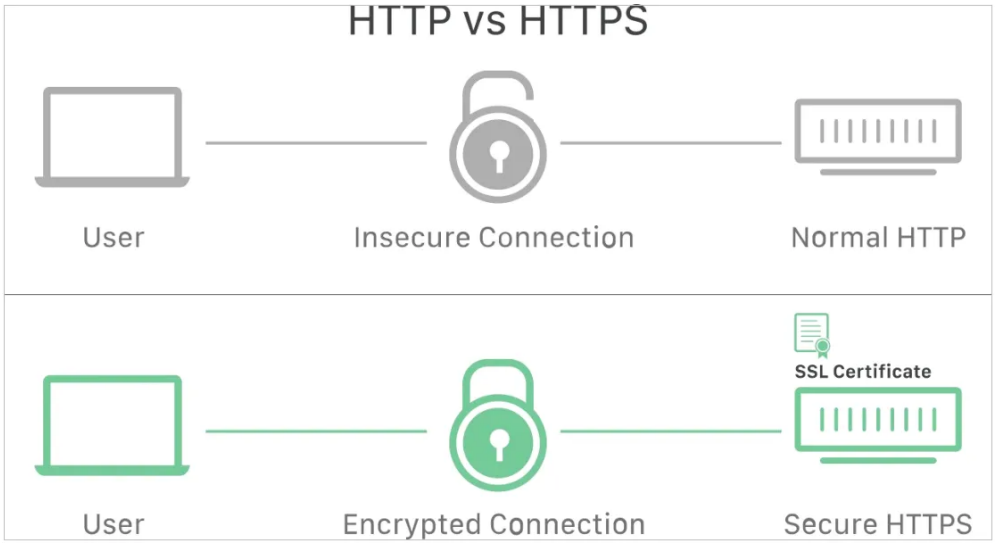

Fig. 1 - HTTP vs HTTPS connection

Comparison of HTTP and HTTPS requests

An HTTP request is just a sequence of lines of text that follow the HTTP protocol.

A GET request may seem like this:

GET /hello.txt HTTP/1.1

User-Agent: cuth/4.29.1 libcuth/4.29.1 OpenSSL/1.2.l glib/1.3.11

Host: www.example.com

Accept-Language: eng

This chunk of text, created by the user's browser, is delivered over the Internet. The difficulty is that it's transferred in unencrypted, which anyone watching the connection may read. (Those inexperienced with the HTTP protocol may struggle to understand this material, but anyone with a basic understanding of the protocol's instructions and syntax may readily read it.)

This is especially true when consumers provide sensitive information via a website or online application. This might be a password, a credit card number, or any other data placed into a form, and HTTP sends it all in plaintext for anybody to view. (When a user submits a form, the browser converts it into an HTTP POST request rather than an HTTP GET request.)

When an origin server gets an HTTP request, it delivers an HTTP response that looks like this:

HTTP/1.1 200 OK

Date: Sep, 12 Dec 2024 11:29:32 GMT

Server: Apache

Last-Modified: Sep, 12 Dec 2024 11:31:01 GMT

Accept-Ranges: bytes

Content-Length: 14

Vary: Accept-Encoding

Content-Type: text/plain

Hello World!

If a website utilizes HTTP rather than HTTPS, anybody monitoring the session may read all requests and answers. Essentially, a malicious actor may read the content of a request or response and determine exactly what information is requested, provided, or received.

The S in HTTPS denotes "secure." HTTPS encrypts HTTP requests and answers with TLS (or SSL), thus in the example above, an attacker would see a string of seemingly random characters instead of the content.

Instead of:

GET /hello.txt HTTP/1.1

User-Agent: cuth/9.72.0 libcuth/9.72.0 OpenSSL/1.1.l zlib/1.3.12

Host: www.example.com

Accept-Language: eng

The attacker sees something like:

G12N+OV/j9p5zLqKEYZnyHDYRyTaladZEXm/0MahBHqnITEzIVRWYhPGW19uITExIUMoU7L1KNn/U7L1KNn/nnHZohMCGMTE71vKEhMTYwIexZHWE

SSL(Secure Sockets Layer)

SSL stands for Secure Sockets Layer, which is a standard for encrypting, safeguarding, and authenticating Internet connections. Although SSL was superseded with an improved protocol known as TLS (Transport Layer Security) some time ago, the word "SSL" is still widely used to describe this technology.

TLS (Transport Layer Security)

TLS is an encryption and authentication system intended to protect Internet communications. A TLS handshake is the mechanism that initiates a TLS-based communication session. During a TLS handshake, the two communicating parties exchange messages to recognise each other, verify each other, decide which cryptographic techniques to employ, and agree on session keys. TLS handshakes are an essential component of HTTPS functionality.

SSL/TLS is most commonly used to secure communications between a client and a server, but it may also protect email, VoIP, and other communications across insecure networks.

SSL/TLS work process:

These are the key proposals to understand how SSL/TLS works:

1. Secure communication starts with a TLS handshake [Fig. 2], when both parties initiate a secure connection and exchange their public keys.

2. During the TLS handshake, both parties generate session keys, which encrypt and decode subsequent conversations.

3. Each new session uses its own session key to encrypt communications.

4. TLS validates the identity of the server or website the user is dealing with. 5. TLS includes a message authentication code (MAC) to prevent data alteration during transmission.

TLS encrypts both HTTP data that users provide to a website (by clicking, filling out forms, and so on) and HTTP data that websites transmit to users. Encrypted data must be decoded by the receiver using a key.

TLS handshake process:

When a user visits a website using HTTPS, the browser initiates a TLS handshake and begins to query the website's origin server. A TLS handshake is also required for any additional HTTPS-based interactions, such as API requests and DNS over HTTPS inquiries. A TLS handshake is a series of messages between a client and a server. A TLS handshake has many phases where the client and server exchange the information needed to complete the handshake and talk. TLS handshakes happen after a TCP connection has been established via a TCP handshake.

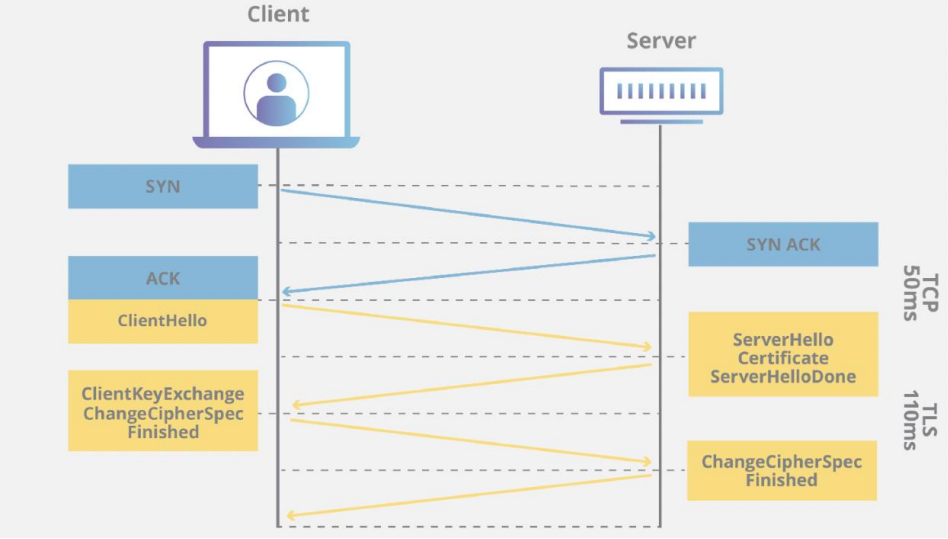

Fig.3 – TLS handshake process

The specific stages in a TLS handshake vary based on the key exchange mechanism employed and the cypher suites supported by both parties. TLS versions prior to 1.3 employed the RSA key exchange algorithm, which is currently deemed insecure. It goes essentially as follows:

1. Client hello: The client sends a hello message to the server. This will include which TLS version the client supports, which cipher suites it supports and a random string.

2. Server hello: The server responds with a message containing: the server's SSL certificate the server's chosen cipher suite and the "server random" a random string generated by the server.

3. Verification: The client checks the server's SSL certificate against the CA that issued it. Then checks the server is who it says it is and the client is talking to the domain owner.

4. The premaster secret: The client sends one extra random string of bytes, the "premaster secret." The premaster secret is encrypted with the public key and can only be decrypted with the private key by the server. The client gets the public key from the server's SSL certificate.

5. Private key used: It ensures the client that the server also decrypts the premaster secret.

6. Session keys derived: The client and the server each derive session keys from the client random, the server random and the premaster secret. They should independently derive the same results.

7. Client is ready: When the client is ready, it sends an encrypted "finished" message using the session key.

8. Server is ready: When the server is ready, it sends an encrypted "finished" message. encrypted using the session key.

9. Secure symmetric encryption achieved: Achieved secure symmetric encryption by completing the handshake and utilising session keys to communicate.

RESULTS

SSL vs. TLS Comparison Table:

Name	**SSL (Secure Socket Layer)**	**TLS (Transport Layer Security)**
Development Alcaide et al. (2020), GlobalSign (2021)	First version was developed by Netscape in 1995	The first version was developed by Internet Engineering Taskforce (IETF) in 1999
Function Mozilla Foundation (2023), NIST (2022)	SSL is a cryptographic technology that employs explicit connections to create secure communication between the web server and the clients.	TLS is a cryptographic protocol that offers secure communication between web servers and clients via implicit connections; it is the successor to the SSL protocol.
Version Imperva (2024)	Three SSL versions have been released: SSL 1.0, 2.0, and 3.0.	Four TLS versions have been released: TLS 1.0, 1.1, 1.2, and 1.3.
Vulnerability Alcaide et al. (2020), Mozilla Foundation (2023), GlobalSign (2021), Imperva (2024)	All SSL versions have been deemed insecure, and therefore have been deprecated.	TLS 1.0 and 1.1 have been declared "broken" and will be deprecated in March 2020. TLS 1.2 is the most extensively implemented protocol version.
Master secret NIST (2022)	The message digest is used to construct a master secret.	A pseudo-random function is utilised to generate the master secret.
Security Mozilla Foundation (2023), GlobalSign (2021)	Less secure in comparison to TLS.	Provides high security

Comparison table of SSL and TLS based on the references:

Reference	**Criteria**	**SSL**	**TLS**

Alcaide et al. (2020)	Overview	Secure Sockets Layer was the first protocol initiated to enable cryptographic security in the network.	It is a successor of the SSL intended to be safer and more efficient.
Mozilla Foundation (2023), NIST (2022)	Security Features	Uses weaker cryptographic algorithms, vulnerable to attacks, such as POODLE.	It makes use of stronger, more efficient cryptographic algorithms, including enhancements of Perfect Forward Secrecy and stronger ciphers.
GlobalSign (2021)	Performance	Generally slower because older, less efficient cryptographic methods are used.	More efficient with better handshake protocols and minimized latencies in TLS 1.3.
Imperva (2024)	Deprecation Status	SSL 2.0 and 3.0 are considered insecure and outmoded.	Deprecating the TLS 1.0/1.1 addition of alerts for resumption and the purpose of early data in TLS 1.2.
Alcaide et al. (2020), Mozilla Foundation (2023), NIST (2022), GlobalSign (2021), Imperva (2024)	Use Cases	Historically used for securing websites and email communications; now largely replaced by TLS.	Widely used for securing web traffic (HTTPS), email, and other communications; recommended for modern systems.
Mozilla Foundation (2023), NIST (2022)	Accuracy	Lower accuracy in terms of security due to vulnerabilities in older versions.	Higher accuracy in security due to improved algorithms and protocols.
GlobalSign (2021), Imperva (2024)	Efficiency	Less efficient due to older protocols and higher latency.	More efficient, particularly with TLS 1.3 which reduces handshake time and latency.

Comparison Table of references:

Reference	**Focus**	**Credibility**	**Accuracy**	**Efficiency**	**Bias**	**Target Audience**
Alcaide et al. (2020)	Technical analysis of SSL/TLS evolution and future directions	High (Peer-reviewed academic publication)	High (peer-reviewed research)	N/A (focuses on historical trends)	Not applicable	Security professionals, researchers
Mozilla (2023)	Understanding SSL/TLS for secure browsing	High (Trustworthy organization)	High (reputable organization)	Low (explains functionality, not optimization)	Potentially favors Mozilla products (subtle)	Developers, general audience

NIST SP 800-52 (2022)	Compliant use of SSL/TLS for federal information systems	High (Authoritative source)	Very High (authoritative government source)	N/A (focuses on security best practices)	None	Security professionals, IT administrators
GlobalSign Blog (2021)	General overview of SSL/TLS advancements	Medium (Commercial source, evaluate for neutrality)	High (security company expertise)	N/A (focuses on evolution, not optimization)	Potential bias towards GlobalSign products	General audience, security professionals
Imperva (2024)	In-depth comparison of SSL/TLS and HTTPS functionalities	High (Cybersecurity company expertise, evaluate for neutrality)	High (security company expertise)	Moderate (compares functionalities, may touch on efficiency)	Potential bias towards Imperva products	Security professionals, IT professionals

DISCUSSION

The Secure Sockets Layer was introduced in 1995. Netscape created it to ensure data security on the internet. SSL has three versions, but only SSL 3.0 gained popularity due to its robust security features.

In 1999, the Internet Engineering Task Force updated SSL 3.0 and renamed it TLS 1.0. The new term was Transport Layer Security (TLS). Since then, we've seen further versions, including TLS 1.2 and TLS 1.3, which is the safest.

Differences Between SSL and TLS Communication Protocols based on tables

1. Protocol versions

SSL and TLS are the encryption methods to communicate over internet. They have many versions, each with different features and improvements. Some of the protocol versions are SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3.

These versions vary in terms of encryption algorithms, key exchange methods as well as vulnerability they fix or introduce.These earlier SSL protocols such as SSL 2.0 and SSL 3.0 have some security weakness which causes them to be open to attacks for instance.

The latest iteration of the protocol like TLS v12(Transport Layer Security) and TLS v13 provides better security attributes including improved ciphers and perfect forward secrecy that ensures enhanced security during transmission of sensitive data through this network channel.

2. Encryption algorithms

The systems of SSL and TLS have many encryption techniques incorporated in them. These are algorithms which control the way data is to be encrypted and protected during transfer.

The Secure Sockets Layer cypher suite has perhaps the most commonly applied technique in SSL. Its algorithms are RC4, DES, 3DES, and AES.

TLS offers new and better encryption methodologies. To begin with, new and advanced encryption algorithms like Advanced Encryption Standard-Cypher Block Chaining, ChaCha20-Poly1305, among others, have been realized due to the Transport Layer Security protocol.

3.Key exchange methods

Key exchange is a vital part of SSL and TLS protocols. They describe ways in which an encryption key is safely exchanged between client, e.g. web browser and the server.

While TLS permits RSA, Diffie-Hellman, Elliptic Curve Cryptography (ECC), even pre-shared keys for key exchange, SSL normally uses RSA or Diffie-Hellman algorithms. Depending on the key exchange technique that is chosen, there would be different implications on how safe the connection whether it's between client and server can be encrypted by means of this method.

4. Security vulnerabilities

In the past, SSL and TLS have both had their flaws in terms of security. Weaknesses in SSL protocols became years ago apparent through poor encryption algorithms and vulnerable key exchange mechanisms. The security flaws exposed by these imperfections can enable hackers to decode confidential data and even carry out man-in-the-middle attacks.

However, there are vulnerabilities associated with TLS compared to SSL. Some cryptographic attacks that affect TLS 1.0 and 1.1 are deemed possible. Such has necessitated the development of subsequent versions including TLS 1.2 and TLS 1.3 which address the security challenges involved.

5. Compatibility and Support

In its sense, the communication over the internet is well standardized in terms of secure communication via SSL and TLS. They are natively compatible with most web browsers and server applications and easily installed for an extra secure layer.

Most of the sites nowadays implement SSL or TLS certificates on the arrival, activating the encryption of the data downloaded by the server through the device of the user. In this way, it secures the most important information from possible unauthorized use.

6. Application in web browsers and servers

Most browsers use the SSL and TLS protocols for secure communications over the internet. Some of the web browsers, like Chrome, Firefox, and Safari, use the SSL/TLS protocol setup to create a secure connection.

Web servers also tend to use SSL/TLS for better security while handling sensitive data. According to this, once the user types HTTPS in the address bar, the website uses an SSL/TLS certificate for secure communication. It activates and encrypts data that can be transferred between the server and the client. To secure the data from getting breached, organisations use the SSL/TLS protocols in web browsers and servers.

7. Impact on website security and trust

SSL and TLS have a huge impact on security and reliability when it comes to websites. Whenever any website uses SSL or TLS the ever-existing connection between your computer and the website is secured.

Encryption makes certain that even if a hacker succeeds in snatching the data, he can't use it because he would not be able to read it. It ensures that you get to or connect to the desired website and are not redirected to any duplicate or phishing site.

As soon as you see https:// in the URL bar and a lock icon, one is assured of a secure connection thereby building trust with the site. Without SSL or TLS, one's connection may be open to attacks which exposes one's information to people who can use it against the person.

References based table

What follows is a sample of available materials to orient you in the confusing jungle of SSL/TLS. The table contains descriptions of the material, for whom it is intended (e.g. beginners, security professionals, etc.), any conspicuous biases (e.g. through a corporation), and the level of truthfulness to expect. All the documents below contain at least something in the way of how efficient the code design is to the question, but none of them treat the question of speed optimisation in any kind of reasonable depth. Use this chart to find the right source for you, whether you want to learn about the basics (Mozilla Foundation), history (Alcaide et al.), how to do it securely

(NIST), what is being worked on today (GlobalSign Blog), or just need to find the best tech for the job (Imperva). Note that you have to watch out for bias, particularly in materials from security companies.

CONCLUSION

The SSL/TLS protocols are simply one of the most significant things you will ever need to have when it comes to data security across the internet. But if you are going to act actively in the Internet space, you should know how these protocols are arranged and take additional ones.

Okay, let's go through this review and we will focus on recent literature literature. It really drives the point of just how crucial it is for one to engage in secure socket layer or transport layer security protocols when communicating on the internet. I will explain what HTTPS is and how it has been growing in usage, how does SSL/TLS encryption work on a low level, what part in overall security system SSL/TLS plays and how it only gets better thanks to constant advances in technology.

However, as this study is our basic research now, there are other things that can be done. Quantum IT and UX are amongst the emerging technological paradigms that should be considered in advancing safe communication. Imitating them, it can provide some helpful information in quite a number of situations.

The SSL/TLS protocols are significant for any Internet user, unless they want to be floored in the middle of the ocean, the 'sea' of the Internet. Well, if you'd like to learn how to safeguard data over the intenet, perhaps you should spare some time and study the best pieces and don't forget to take the quizzes. It is also crucial to add that there is no end to security and know ledge is indeed valuable when it comes to internet identity.

REFERENCES

[1] Alcaide, A., Alonso, F., Lopez-Hernandez, J. C., & Gonzalez-Tablas, J. M. (2020). A historical look and future trends in SSL/TLS. Security and Communication Networks, 13(24), 6077-6090. Hindawi Limited.

[2] Mozilla Foundation. (2023, May 17). How does SSL/TLS work? Mozilla. https://developer.mozilla.org/en-US/docs/Web/Security/How_does_SSL_TLS_work

[3] National Institute of Standards and Technology (NIST). (2022, December). Special Publication 800-52 Revision 2 - Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-52). National Institute of Standards and Technology.

[4] GlobalSign Blog. (2021, February 19). The ongoing evolution of SSL/TLS. GlobalSign. https://www.globalsign.com/blog/ongoing-evolution-ssl-tls

[5] Imperva. (2024, February 12). SSL/TLS vs HTTPS: A detailed comparison. Imperva. https://www.imperva.com/blog/ssl-tls-vs-https-detailed-comparison

[6] Shaymaa Adnan Abdulrahman, Bilal Alhayani,A comprehensive survey on the biometric systems based on physiological and behavioural characteristics,Materials Today: Proceedings,Volume 80, Part 3,2023, Pages 2642-2646,https://doi.org/10.1016/j.matpr.2021.07.005.Alhayani, B.A., AlKawak, O.A., Mahajan, H.B. et al. Design of Quantum Communication Protocols in

[7] Quantum Cryptography. Wireless Pers Commun (2023). https://doi.org/10.1007/s11277-023-10587-x

[8] B. T. Sabri and B. Alhayani, "Network Page Building Methodical Reviews Using Involuntary Manuscript Classification Procedures Founded on Deep Learning," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-8, doi: 10.1109/ICECCME55909.2022.9988457.

[9] Omar A. AlKawak, Bilal A. Ozturk, Zinah S. Jabbar, Husam Jasim Mohammed,Quantum optics in visual sensors and adaptive optics by quantum vacillations of laser beams wave propagation apply in data mining,Optik,Volume 273,2023, Ismaeel, N.Q., Mohammed, H.J., Chaloob, I.Z. et al. Application of Healthcare Management Technologies for COVID-19 Pandemic Using Internet of Things and Machine Learning Algorithms. Wireless Pers Commun (2023). https://doi.org/10.1007/s11277-023-10663-2.

[10] Mohanty, Niharikaa | Pradhan, Manaswinia | Mane, Pranoti Prashantb | Mallick, Pradeep Kumarc; * | Ozturk, Bilal A.d | Shamaileh, Anas Atefe : Intelligent Decision Technologies, vol. Pre-press, no. Pre-press, pp. 1-26, 2024

[11] Rane ME, Bhadade US. Multimodal score level fusion for recognition using face and palmprint. International Journal of Electrical Engineering & Education. 2020;0(0). doi:10.1177/0020720920929662