BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 03, Juni-Juli (2022)
ISSN 2829-2049 (media online)
Hal 523-538

Evolution of Cryptographic Techniques: Overview of the Existing Approaches and Trends of the Development

Noman abid

American National University USA

nomanabid12345@gmail.com

Abstract

Cryptography remains to be one of the oldest and indispensable principles of today's information protection disciplines because it gives indispensable tools for protecting content and messages during the communicational and data transferring actions. This review surveys extant research on possible cryptographic methods and their applications in different fields comprising of conventional key-based and new-complexity key based cryptography, cryptography based on Block chain, Homomorphic Cryptography, Post Quantum Cryptography and other types of cryptography. New complicated threats, emergence of Quantum computing, AI, block chain, and 5G, IoT are posing new threats and challenges and opportunities in cryptography. In this paper, some of these areas to key issues include: problems such as vulnerability of the traditional cryptographic system to brute force attacks, the impact of new developments in quantum computing to current encryption security systems, and the problem of key management, and side channel attacks. This article addresses how cryptography is used in protecting emerging technologies such as how light weight cryptography is incorporated to IoT peripherals, how works cryptography is applied to block chain or crypto currencies, and artificial intelligence systems. While with the arrival of quantum computing capable of threatening the security of classical cryptographic methods, the focus of the cryptographic community shifts to post quantum options like QKD and lattices. The next section of the review also talks about directions for future development direction of cryptography, and emphasizes the importance of creating new cryptographic algorithm that caters for the demand of scalability efficient and security to meet the increasing development in technologies. Cryptology is still needed for protection of relevant information and for proving secure communication for the age of integrated and computer-oriented society. The further evolution of intricate cryptographic methods and their integration into the advanced technologies is useful to combat new threats and guarantee safety of information that is to be necessary in the following years.

Keywords: Cryptology, SKC, AKC, HC, PQC, QC, Block chain, IoT, 5G Networks, AI, KM, DAA, DS, QKD, LPA, CA, DC, S, Cryptographic Protocols

INTRODUCTION

Cryptography- the technique of executing confidential communication and information is one of the basic crannies which forms the basis of current cybersecurity. Its main purpose is to store an organization's most important or sensitive data so that only specific individuals can access or modify it. However, cryptographic methods have risen over the ages to an extent that the ages of aligning old ages with modern technology, security needs, and threats processes. As mentioned before, in its most basic application cryptography was only used in early civilization for military and diplomatic purposes [1]. The above-mentioned first methods of enciphering, which has been in practice in the ancient ages, are as follows: – Caesar cipher Where the languages in the alphabet messages are shifted. Going to the next level of the civilization, it becomes even more refined to evolve different cryptographic methodologies and with special reference to the improved numerical computation technologies of the twentieth century. As the development of modern computer systems and the internet took place cryptography became a much more important place. Now, such cryptographic method is necessary for a person's data security, monetary transactions, information exchange, and state protection. The possibilities of e-commerce, online banking or digital communication have arisen the demand twice as great as a protocol, and cryptography serves as a basis for every one of them [2].

RSA is undoubtedly one of the most important revolutions that ever happened in latest cryptography world. Published in 1976 Whitfield Diffie and Martin Hellmen made public key cryptography massively popular in security as it provided the opportunity to individuals to share information via insecure channels without having to exchange the private key before. It led to the creation of the so called now 'crypto algorithms' starting with the RSA algorithms and all the way to Elliptic Curve Cryptography (ECC). Cryptography is not more a simple method of encoding and decoding messages. They now encompass digital signatures, hashing algorithms and cryptographic protocols all of which play different roles of data identity, genuineness and secrecy [3]. For instance,

you employ hash functions like SHA-256 for applications like digital certificates and block chain technology on which integrity of the information being protected is imperative.

Thus, it cannot seriously be doubted that there is a role for cryptography, and this conclusion may be arrived at without the aid of any of the various theoretical assumptions. It directly impacts on participation in the society, and how man handles this necessity daily. Whenever user inputs credit card number, or any other person's identity details, the cryptography guarantees the safety of data input. Encryption is like the same when in a position to type emails or even making that video calls; it ensures that the information passed is supposed to remain between the two parties only as planned without third party eavesdropping. However, there are some problems which cryptography, an apparently foundational subject – or the application of strong theory to bromidic practice – meets. It appears that insecurity has continued to grow over the years as the basis for the underlying technology is also changing? Modern cryptography is endangered by the developed computational abilities of present day computers and particularly prospective quantum computers of the future [4]. Therefore, further study focuses is made on the development of new methods that are resistant to these newly appeared threats: post quantum cryptography this process is intended to safeguard information from such quantum computers.

The current review constitutes a survey paper on the historical development of cryptographic methods and on the state-of-the-art methods that are being developed at the current era. The goal of this paper is to look at the current state of development of cryptography and possible prospects of its further growth in order to gain a deeper understanding of how this vital sector defines the nature of the information security in the constantly developing and integrating environment. In this discussion, both sides of the modern cryptographic forms shall be discussed to provide a rich information treatment of this fields, which is still expanding [5].

EVOLUTION OF CRYPTOGRAPHY

It is realized that the study of cryptography has been done as soon as there was need for secret communication. It was foresee used as a secret message use was significant in the military and diplomacy above all before and during the combat. Cryptography has been slowly progressing for centuries from methods completed mathematically by hand to those systemized now. This evolution of the product is characterized by certain important events that are linked with the evolution of technology on the one hand and the growth of the complex in threats to security on the other.

Early Cryptography: The formative signs of cryptography are far as early as the classical period of early societies. The first types of cipher are some of the easiest to perform and among the types documented and being used today is the Caesar cipher. This cipher was a kind of substitution cipher, whereby each and every character in the text is shifted by fixed number of positions in the alphabet. Yet it was simple, and it was the first time in the history of mankind that attempt had been made at obliterating any possible way of the leakage of information to the wrong quarters. Subsequently, the scale cipher which is said to have been used by the Spartans in the 5th century, BC involved revolution of a strip of parchment round a cylindrical torso [6]. The text would be written along the length of the cylinder and only individuals having own cylinder can read it. These are the early cryptographic methods as much as they could be easily compromised with more basic techniques for what was in actuality a comparatively restricted setting.

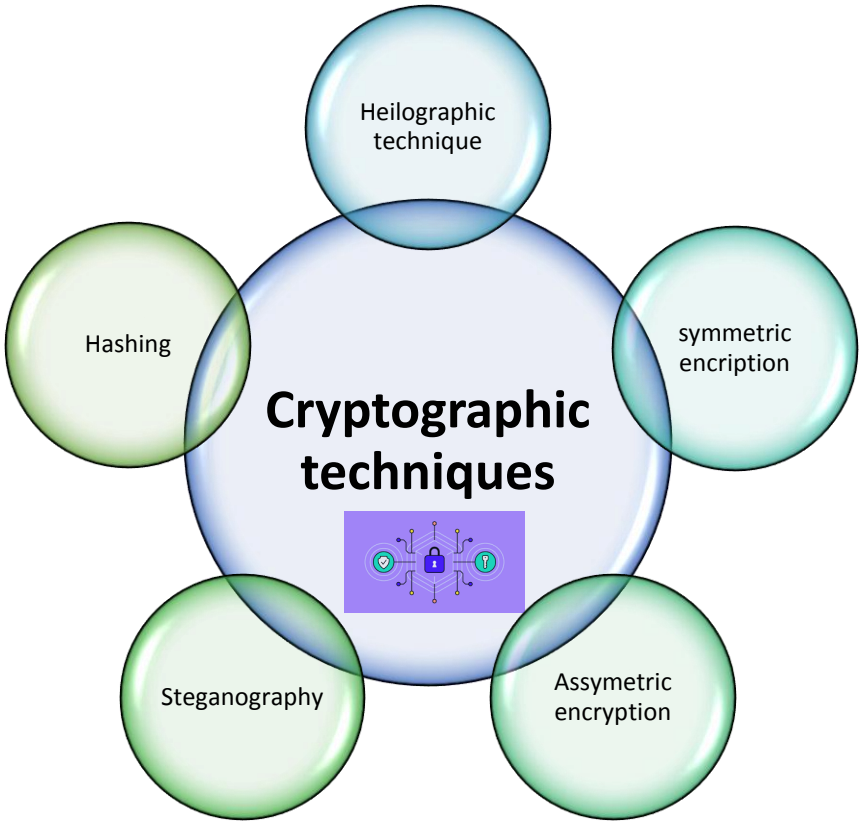

Figure: 1showing cryptographic techniques

Other early category of ciphers was likewise invented in the period of Middle Ages but enhanced later. Among the latter, there was an outstanding one of the 16th century the Vigenère cipher created by Blaise de Vigenère. They adopted a polyalphabetic technique in which a keyword was used to decide on the shifting of the alphabet than the previous technique. However, as was seen throughout this paper, with the help of cryptanalysis, quite a number of the classical ciphers were decrypted in the end. The twentieth century saw growth of Cryptography within a very short time given the development of computers as well as secret communication especially during warfare. Enigma a cryptographic machine that the Germans used during the Second World War is undoubtedly one of the most popular cryptographic machines [7]. It employed rotor-based encryption – which appeared to be difficult at first to crack and which was almost impossible to penetrate. Nonetheless, those cryptographic officers, specially the group lead by Alan Turing, unlocked Enigma messages which was one of the key factors how Allied forces triumphed over WWII.

The most significant evolution in cryptography in modern world was started in 1976 when Whitfield Diffie and Martin Hellman started using public key cryptography. It offered a concept that perceptive secured communication between two parties who have no prior dealings with each other and who am unable to share secret key. What happened here though is that there was only one key to encode the information, and there was another to decode it (public key and private key respectively). Nevertheless, the clear indication of the feasibility of public key cryptography introduced by Diffie and Hellman in 1976, but only RSA published in 1977 which the first-known public-key algorithm is made it possible [8].

In point of fact, public-key cryptography became the foundation of the modern methods of encryption and complex protocols which, in their turn, uninterruptedly guarantee the security of digital communication, bank operations, and commerce. On the other hand, symmetric key established foundation in data encryption till date with depending and then moving up in a single step securely transporting data in transit with DES and AES. As the performance of computers was enhanced, the intricacy of the cryptographic methods rose to match them as did the cryptanalytic skill. Hash functions including, MD5 and SHA added on extra security mechanisms through which not only data could be encrypted but details relative to the authenticity of data were easily checked to show the accuracy of the data in regard to its origin and any changes that may have been made on the material [9]. A digital signature ensures that the content of the message has not been changed in transit and hash functions ensure that content has not changed while in transit or while stored in the database.

The transition to the Internet and digital communication at the end of the twentieth and the beginning of the twenty-first century again and again brought attention to the need to create even more reliable cryptographic methods. Web security and Ip security technologies in particular SSL/TLS and IPSec respectively got useful in achieving confidentiality, integrity, and authenticity of information being conveyed through internet. Studying the history of cryptography learned that there was always evolution in the manner information was being protected. Seeing that cryptography was initially required in an effort to shield communication from prying eyes it has evolved over time in much the same way as the need for security and the enemies. Moving into the future of digital communication based on computers and the Internet, we realize that the tradition of the first steps in cryptographic methods has founded ideas for creating the modern systems of security [10]. All the data needs to be encrypted and there are two approaches to encryption of data: Traditional and integrated encryption techniques IESM/3F Class notes IESM/3F Class notes Encrypting Data There are traditional and integrated encryption techniques The Clash of Small Arms Fire with Advanced Combat Helmets

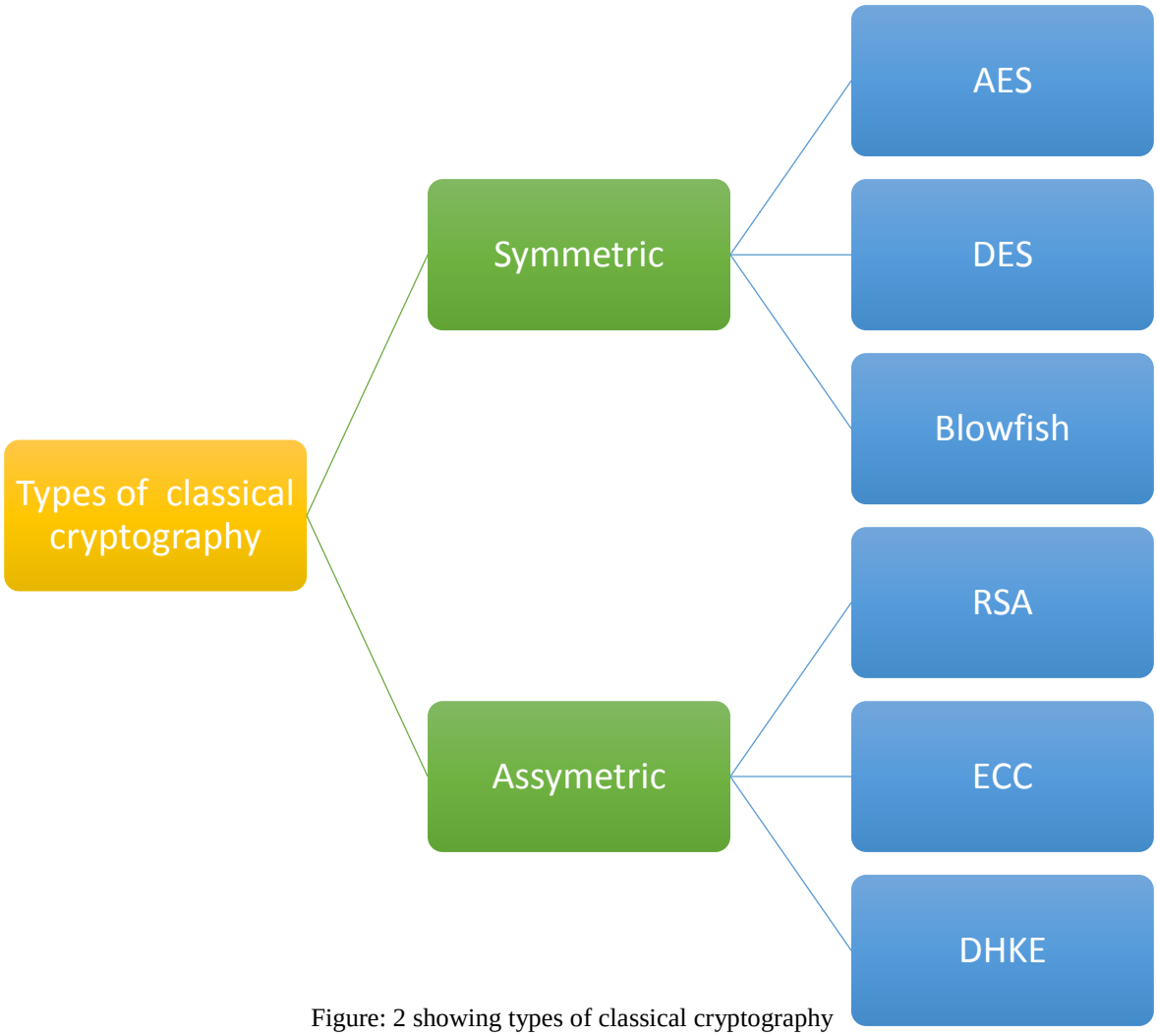

Figure: 2 showing types of classical cryptography

Randomized numerical formulae are some of the earliest approaches that have been employed to define the current forms of the practice. Originally, these techniques were designed for relatively primitive forms of message interchange that formed the basis for today's complex structures. Conventional cryptographic techniques are largely associated with symmetric secret key cryptography where even the decryption key is actually the key for encryption. However, these algorithms are not enough secure for the modern world though they are very important for understanding how cryptographic practices evolve [11]. The basic principle of the classical cryptographic algorithms is the symmetric key cryptography with the meaning of the identity of the key for the decryption of the message – key and for the encryption of the message – key. As with symmetric, a quadratic approach is used, ultimately offering the great result in employing much information transferred. However, their major weakness stems for instance, transmission of the key from one party to the other, because anyone who gets the key, in real sense decipher the messages.

Data Encryption Standard (DES) is viewed as one of the most representative examples of the application of the symmetric key algorithms in the twentieth century. DES was developed by IBM in 1970s and NIST at later time, it used a 56 bit key for encrypting 64 bits. It was previously believed to be safe for the time for which it was invented but with the new improvements in the computing processing this became vulnerable to a brute force attack. Many of DES was eroded with the exhaustive search methods adopted in the 1990s, and as a consequence, most of it was dehydrated [12]. DES was then followed by the Advanced Encryption Standard (AES) which – at least for now – is one of the most widely used encryption standards in existence that was developed in 2001. AES processes the data in 128 bit data blocks and has fixed three key sizes of 128, 192 and 256 bits. It uses substitutions, permutations and mixing for the purpose of safe transmission of the data that has to be sent over the internet. AES has been used widely in several field including the web security through the Virtual Private Networks (VPNs) or SSL/TLS, security of storage data and protection of financial transactions.

However, the use of the asymmetric key cryptography raised the entire practice of the cryptography to the mid-20th century or modern cryptography. Asymmetric cryptography uses a pair of keys: The function of converting plain text into cipher text is performed by an encryption key called public key; the key that decrypts a cipher text is referred as the secret key. In this approach, there is no need of pre-sharing keys and therefore makes it easier for two strangers to converse securely. This paper aims at reviewing the RSA algorithm, which is among the most outstanding conceptions in asymmetric cryptography invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977 [13]. This is all the security that RSA employs – the qualities of big two prime numbers and factoring them. This makes it possible to transmit the information via an untrusted channel while making it the foundation of numerous secure connection protocols. RSA has uses in various forms in various systems such as in digital signatures, emails and key exchange secure.

Diffie Hellman key exchange another prominent asymmetric cryptographic algorithm well known method developed by Whitfield Diffie and Martin Hellman in 1976. The difficulty of Hellman does not enable encryption but enable one jurisdiction to securely exchange a secret key with another in an open network. It lies on the fact, which is mathematically complex for the adversary to solve, discrete logarithm problem on finite field, so the eavesdroppers cannot discover the secret key [14]. This algorithm is being used as a building block of most safe communication systems for instance SSL/TLS used in protecting internet traffic. Hash functions are such another important element of classical cryptography. A hash function is a function that receiving informa¬tion (or a message) transforms it into another, equal and determinate, code length (termed the hash value or digest). The output map is not affected by any of the processes or inputs; it is expected that, for any minor change that might be made to the input, the hash value will be very different. These are in the use of digital signatures, and the message integrity checks. One of the world's most popular hash functions are in the SHA-family (Secure Hash Algorithm); SHA 256 is primarily used for data integrity and all other relevant use in line with cryptography as for example the block chain [15].

Electronic signatures based on a hash function and an asymmetric key cryptography, thus allowing verification of a message's authenticity and message content. That how digital signature works is that a private key is applied on the Hash of message. In terms of signature the theory is that whoever gains possession of the corresponding public key of the sender will in fact be able to verify that he/she is the rightful owner of the signature, that is, the message was not tampered with and that it came from the right source [16]. Digital signatures are a name that comes in the use of many options such as software distribution, legal papers & documents, and in the case of email authentication. However, as it will be shown further, the majority of the classical cryptographic algorithms is replaced by the new and much more effective ones, still classes of these algorithms are still the foundation for the formation of the modern encryption production. Mirrored algorithms that exist today are the Advanced Encryption Standard (AES); the asymmetric are RSA and the Diffie-Hellman technique put a lid on safety going to the digital front. In addition, classical algorithms are still relevant in the study and training in cryptology because many complicated structures are built on top of it [17].

The weaknesses of the sort that were identified in such older algorithms as DES were the facts that made such people look for better and more efficient systems of encryption and one of the above results of such a search is AES. Similarly, use of key exchange protocols such as the applied Diffie-Hellman still is deemed to necessitate the construction of safe communication protocols. Present day cryptosystems are built on the basis of classical cryptographic algorithms including the symmetrical key algorithms, asymmetrical key algorithms and the hash functions [18]. It cannot be overemphasized because they formed the basis upon which the earlier processes were developed for creating the secure means of communications we use in the present.

BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 03, Juni-Juli (2022)
ISSN 2829-2049 (media online)
Hal 523-538

ADVANCED CRYPTOGRAPHY SYSTEMS

In recent years novelties attached with the classical algorithms of cryptography have come into picture and are being used because of the complexity and requirement of the modern day's communication. It is claimed that they are best used where strong security protection is required in spite of smarter attacks and modern technologies. The development of a rapidly emerging computational capability, the opportunities for internet communication, and the quantitative computing danger all call for improving cryptographic techniques [19]. The most frequently used postmodern cryptographic algorithm of the present generation is the Advanced Encryption Standard commonly referred to as AES. It was decided that AES should perform the DES's role because AES is safer and performs better than als. AES work on a fixed block size of 128 bits and the key size can be of 128, 192 or 256 bits. A type of data transformation is a sequence of operation, which uses substitution, permutation, and mixing for data encryption and decryption. AES is applied for security of information in governmental and non-governmental organizations and for banking and the other companies [20].

Nevertheless, different threats have come to the fore and therefore cryptographic researchers have never stopped in search of new AES replacements. For instance, the identification of optimization problems involving the protection of quantum techniques from quantum machinery has led to an extensive discussion of post-quantum cryptography or PQC designed to withstand quantum computation. Another two more recent revolution of modern cryptography are aptly known as based on one of a kind known as Elliptic Curve Cryptography (ECC). ECC on the other hand uses elliptic curves' mathematics to construct more efficient keys than traditionally used in RSA or indeed any other PKI systems. However, to fully understand the advantages of using ECC the following points must be taken note of more specifically, the above-said proposed technique can attain the same degree of protection with shorter keys than the required amount of time and memory [21]. For example, ECC key of a security level of 256 is comparable to RSA of 3072 bits. Such efficiency of ECC makes it suitable to be used in an environment that has stringer limitations to those of mobile systems, that of IoT systems for example.

It's finding use in application protocols like TLS and SSL to present rapid and secure encryption for Web information transfers. It also becomes standard in other products like the crypto currencies for instance the Bit coin and Ethereum where it is efficient in indicating the importance genom validation of the transactions as well as the security of the network [22]. As with the appearance of the idea of quantum computing it has been for the most part considered that it will be able to make many of the basic algorithms irrelevant or, at best, quite inefficient particularly those which are predicated on factoring large numbers as in RSA and discrete logarithms as in the Diffie-Hellman. Those cryptosystems can be however vulnerable to attacks from quantum computers using Shor's polynomial time algorithm in factoring large numbers. Therefore, there is a threat in the case of success of quantum computing, specifically, this has stimulated emergence of a new field of study called Post Quantum Cryptography (PQC). As an effort to lay the foundation of PQC, PQC is supposed to develop cryptographic algorithms which resist quantum attacks. There are some promising candidate PQC algorithms: Lattice structure based, code structure based, hash structure based signatures. But what is important here is that all the cryptographic schemes described above do not rely on the mathematical assumptions that can be used by the quantum algorithms, which makes it a viable candidate for post-quantian security [23].

One of the relatively recent advancements in the modern area of cryptology is homo morphic encryption. As for other method for securing data, computations over the data are performed in plaintext, having the data decrypted first is a disadvantage of the Homomorphic encryption however allows computations to be made on encrypted data without the need to decrypt before this. This had the implied meaning that for example, viewpoints or otherwise sensitive data can be safely processed in a cloud or otherwise third-party platform and yet the actual data is never actually shared [24]. Homomorphic encryption definitely has a very broad applicability in areas such as secure cloud computing and personal computation and data analysis. Though it is expensive and by no means real time, has the current research focus been on attempts to optimize the extraction process for actual application.

Advent of block chain technology has brought new dimensions in application of cryptographic technique especially in aspects to do with security of transactions and integrity of data in distributed environments. Block chain employs use of cryptographic techniques such as hashing functions and digital signatures to safely store as well as make transactional data noticeably accessible in the node-based networks [25]. Cryptography hash, for example SHA-256, is useful in production of unique identification number for blocks of data in the network while digital signature is useful in attesting to the validity of transactions. The decentralised structure of Block chain eliminates the use of middlemen for ensuring trustful transactions, which has created opportunities for functional peer to Peer transactions, crypto currencies, and smart contracts.

Cryptographic protocols are in fact frameworks that state how cryptographic algorithms are implemented and used for the purpose of communication security. These protocols guarantee that data is concealed, is from the right source, and in the right state during transmission between two parties even when there are extraneous interlopers. Cryptographic protocols have become very essential for securing several forms of communication such as emails, banking and transactions, data exchange within networks etc. A popular cryptographic protocol is Transport Layer Security (TLS) and is used to protect communication over the internet. TLS is the newer concept after the Secure Sockets Layer (SSL), which the primary function is to offer privacy between two applications that are communicating. If you use HTTPS to access a Website, TLS is also in charge of encrypting the client-server information exchange to safeguard such important data types as the passwords and credit card numbers [26].

The TLS utilises both the symmetric and asymmetric encryption mechanisms to form a secure link. The process starts with an exchange of keys by public key authentication of which RSA or ECC is most commonly used to authenticate the shared secret. Once the key exchange is completed, what is known as 'session key' is applied over session for authentic symmetric encryption algorithm such as Advanced Encryption Standard (AES), in order to achieve a fast transfer of data without compromising on security. Other key protocol is Internet Protocol Security (IPSec), responsible for network layer communications security [27]. As a protocol, which offers protection of IP packets to encompass encryption, authentication and integrity, IPSec can be crucial to Virtual Private Networks (VPNs), secure data transfer and the protection of private networks implemented over generally accessible means such as the internet.

Two of the important components of security are authentication and authorization and several protocols have been designed in order to provide the user with adequate protection along with privacy while using the resources. OAuth is an authorization framework that provides small application permissions to access a user's data without having to use his/her login details. OAuth is used mostly in services such as social media since an application can directly request a user's profile or data from other services without additional exposure of passwords. Another protocol for authentication to mention is SAML (Security Assertion Markup Language) that is widely used in enterprise. SAML is designed to provide Single Sign-On (SSO), you sign in once on an integrated system to avoid signing in to multiple systems. SAML stands for Security Assertion and Markup Language and it also works with two parties, one is Identity provider and the second is service provider and here story exchange between two parties occur via XML-based asserts to authenticate the parties and services [28].

Cryptographic protocols have been induced in modern societies as block chain technology has emerged to be marker of secure decentralized systems. The block chain relies on cryptographic hash (for instance, SHA-256) for the authenticity of the transaction data and to protect the ledger. Electronic signatures are applied to confirm the identity of transaction; and consensus protocols like PoW or PoS make sure that all nodes on the network have equal perception of the transaction history. As in any block chain-based systems, there is no need for a central authority to authenticate or validate the transaction because the cryptographic protocols take care of the trust required between two parties [29]. Due to this, the use of block chain has become rampant in crypto currency systems such as Bit coin, Ethereum and other smart contracts and decentralized finance (DeFi) applications. The cryptographic protocols make practical use of cryptographic techniques with emphasis on communications, authentication, and distributed systems, thus are core to cybersecurity. In future, due to the advancement in technologies and new threats, the cryptographic protocols will become more intricate to maintain the secrecy, accuracy and non-repudiation of the communication [30].

USES OF CRYPTOGRAPHY IN CURRENT WORLD

Cryptology is at the core of today's global digital security and is applied to anything from mere text messaging to banking and other financial transactions. The uses are numerous and extend to penetrate almost all sectored in our daily existence. With the enhancement of the digital technology it is a matter of urgency to implement effective cryptography to enhance security of information and provide privacy and trust in the digital environment. Another common use of cryptography is in guaranteeing security of lines of communication [31]. We have seen many application-layer protocols such as WhatsApp, Signal, and Telegram where messages transmitted between individuals are encrypted at both ends (end-to-end encryption) so as to make the third party including the service provider not to read the messages contents which are only understood by the sender and the receiver. It is done by using techniques like AES on the contents of the message while RSA or ECC will for the exchange of such keys.

In the same manner, PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions) are meant to encrypt the privacy of an email message as well as its authenticity. For instance, PGP employs symmetric encryption for the actual message, as well as asymmetric encryption when it is necessary to encrypt keys, so only those intended can open the e-mail [32]. Crypto graphy is critical in the security of other financial transaction,

specifically internet payment and banking systems. In digital banking, credit card transactions and online payments, cryptography shields ordinary data such as account numbers and identification information. For instance, in online shopping, personal details such as credit cards and address details are protected through SSL/TLS where information's exchanged between the buyer and online merchant are encrypted [33].

Cryptographic algorithms are also used in digital currencies such as Bit coin, Ethereum, and the rest. Applications like the crypto currencies themselves utilize cryptographic principles like hash algorithms for instance SHA-256, digital signatures among others to secure the different transactions while keeping the integrity of the online block chain ledger intact [34]. Ownership of crypto currencies is transferred securely using public-key cryptography, while miners employ cryptography to solve puzzles and thereby incorporate transactions into the block chain. Students learn that as the issue of privacy emerges, cryptography offers methods of securing an individual and a company's information. Full disk encryption systems, for example BitLocker that is a Windows hardened disk protection system and FileVault that is a Mac OS operative system hardened disk protection system encrypt files and disks. Sitting with the device as it is misplaced or stolen, the data cannot be retrieved because of the encryption process.

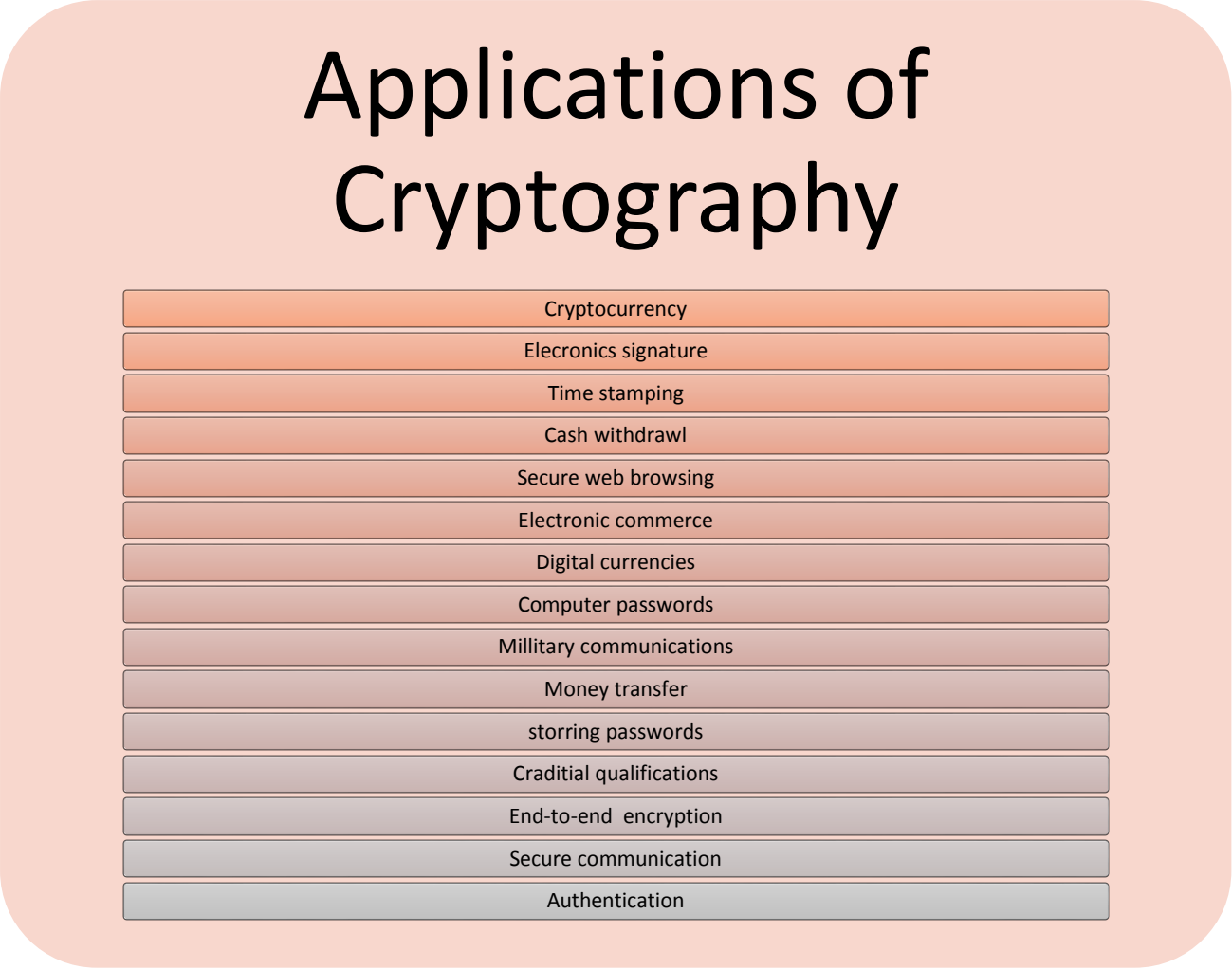

Figure: 3 showing applications of cryptography

Services such as Google Drive, Dropbox or iCloud incorporate cryptographic protocols to protect the user data, during the transmission and while waiting in storage. Effective encryption also means that no one gets access to the end user's files except the end user himself/ herself including cloud providers [35]. The other area of data privacy is anonymity and this Tor (The Onion Router), advanced through cryptography makes it easier. Tor is used by its users to browse Internet anonymously, encapsulating all the traffic and forwarding it through a huge network of volunteers relaying data for the user to conceal identity and location. Being at the center of protection of information, governments and military organizations are among the key consumers of cryptography. Secure information transfers and upholding of security matters of countries involve the use of secure codes, techniques

known as cryptography. Encryption procedures used by satellites are taxed on a military standard to protect satellite communication, intelligence, and diplomatic information from enemies.

Also, PKI can also be used by governments in providing digital signatures, identify citizens and secure online services, file taxes and even to vote online. Employment of cryptography in e-governance makes the accessibility of government facility secured and also the data cannot be altered. Due to the advancements in telemedicine and healthcare data management, the existence of cryptography is indispensable as it comes to the protection of patients' information. Health information should be protected by law in many countries and there are certain laws in every country which protect patient's privacy of data like HIPAA in USA [36]. Sencryption is applied to safeguard medical records as the PHR data can only be accessed by other healthcare practitioners. Also, personal and sensitive information exchange in patient-doctor and doctor-hospital, strongly utilizes cryptography procedures. For instance, the new FHIR (Fast Healthcare Interoperability Resources) and other emerging healthcare standards incorporate encryption for the privacy and integrity of information in the healthcare systems while in transition from one system to another.

Cryptography also plays vital role in managing safe digital identities and healthy methods to authenticate user mostly in online services. Implementations of two-factor authentication (2FA) in online platforms (including banking, social networking, e-mail) are widespread The idea of 2FA is that the user proved to know something (like a password) and also possess something (a time-specific short pass code which is sent to the user's number or generated by Google Authenticator). Another cryptographic technique which is useful for managing identities include public key infrastructure- PKI. PKI systems involve the use of two keys, a public key and a private key in authenticating parties to transactions in computer based deals. The usage of authentications from reliable CA assists to confirm the bona fide nature of the user or the website besides endorsing that the communication is safe [37].

With the increased connection of IoT devices, new security concerns have emerged, more so, on how to secure the interactions between smart devices. Encryption is employed broadly in IoT security mainly where the information shared between linked devices and the principal host server is secured against foul play. For example smart devices in smart homes such as smart thermostat, home security cameras employ cryptographic systems in an endeavor to safeguard all user data as well as also to ensure that the IoT devices can only connect to other devices that are allowed. Nowadays cryptography helps to maintain the authenticity and confidentiality of digital voting systems in most democracies [38]. Voting is highly secured through encryption and digital signatures so that no one's vote is disclosed to the other party and most importantly, votes are not duplicated. Use of cryptography enables checking of fraudulent activities within the election procedure and the entire process is secured even when voting is done through electronic means. Cryptography has turned into a necessity to go round the world which protects data communication, privacy, identity, and commerce. Cryptography will remain relevant in the defense against new threats as technologies progress in digital space and as people rely on digital systems. From protecting personal identity information, electronic funds transfer, privacy in telemedicine or e-health, and government and sensitive information security, cryptography is the basis for today's computer security.

SOME QUESTIONS AND ISSUES IN CRYPTOGRAPHY AND PERSPECTIVES FOR THEIR SOLUTION

Cryptology plays a significant role in securing computer and digital communications however in current STEM there are challenges that arise. These ones emanate from different grounds ranging from advancement in computational abilities, emergence of new form of attacks, and other issues like emergence of quantum computing among others [39]. To be capable and be able to serve its purpose cryptography must overcome these challenges and that is why with new arising issues research is still being conducted to find ways, tools and approaches to counter them. This section looks at some of the major issues facing cryptography today and presents some possible future avenues for the subject.

The only limitation to breaking traditional cryptographic algorithms is the ability to measure up to the enhancements in the computational power. This is the most general technique that an attacker uses in order to decipher a cryptosystem, in that they will endeavor to try out all possible keys until the right one is arrived at. While cryptographic algorithms are continually becoming more robust, the cost of producing hardware to implement an exhaustive search on many candidate keys is decreasing relative to the cost of developing a brute-force mechanism for some algorithms as the key sizes of the latter are not as large. For instance, RSA algorithm is prone to attack if its key size is tapered off. In due course, the cryptographic community has suggested the use of larger key sizes, such as 2048 or 4096 bits for RSA, but due to ever increasing processing power these as well may

cease to be sufficiently secure. As a result, cryptography researchers are attending to discover new algorithms and systems that are strong enough to opt for with these superior brute-force attacks [40].

The greatest threat over current cryptographic systems in the future is quantum computing. Quantum computers use mechanics to solve computations that can otherwise be solved by normal computers or cannot be solved at all. Algorithms like Shor's algorithm are really dangerous for public key cryptographic techniques such as RSA and ECC. These algorithms depend on the facts that the quantum computers provide superior performance over the classical computers in math computations especially the factoring very large numbers and solving off known logarithms very fast in extremely short time that can potentially render the existing encryption solutions as insecure [41]. To counter this threat the discipline of post-quantum cryptography has been created. PQC expects to create cryptosystems that cannot be vulnerable to adversarial quantum analyzing. Some of the future research directions include Lattice-based cryptography, code-based cryptography and Multivariate Polynomial Encryption. Nevertheless, PQC is currently a work in progress, and it may take a few years before its implementation and distribution of quantum-resistant algorithms are fully set.

A powerful threat is side-channel attacks – these are attacks exploiting physiological parameters of cryptographic HW/SW to decrypt data. "These attacks do not try and penetrate a specific mathematical flaw in the algorithm that underpins encryption, but will instead exploit other subtle signals given off during the encryption process; normally power consumption, electromagnetic or indeed time differences." For instance, they are capable of evaluating the time it takes in an encryption operation to determine secret keys. Side-channel attacks therefore poses serious threat in areas where cryptographic keys are securely stored in devices like smart cards, HSMs and engineered systems. Side-channel attacks require means to leak out information from cryptographic systems and therefore, such systems and their algorithms require protection based on counter-features, including constant-time execution of algorithms, noise addition or a shielding of physical space [42].

Key management is certainly one of the most significant factors in cryptography out there. In symmetric keyword the same keyword is used for encryption and decryption. The main issue is to protect the distribution and storage of these keys and to do so when running over environments that might be observed by an attacker. The weakness of the method is that if an attacker gets the key, then the method of encryption is rather useless [43]. Public-key cryptography only alleviates this issue by facilitating key exchange over an insecure channel key distribution and establishment remained a problem especially for large scale applications or in systems with thousands or millions of users that require secure key management. The problem that organizations have when it comes to keys is the generation, distribution, storage, and even revocation of the keys in a way that will not expose the organization to attackers. One such answer is key management systems (KMSs), which concentrate on the creation, distribution, and storage of the crypto keys. Thus, their protection and further upgrade is still a problem, with regard to which big-scale and distributed platforms, for example, IoT, are of great concern [44].

There is also a critical tension between efficiency and sustainability if it relates to cryptography. High quality cryptographic solutions may entail considerable resources, and this is a significant limitation to the current generations of devices especially with either limited processing power or memory. For instance, operations in big amounts of data with the help of algorithms like RSA or performing homomorphic encryption will take time to be done and will slow down the system. In IoT devices, mobile devices, and embedded systems, there is always this quest for high performance cryptographic algorithms that will give sufficient security with minimal impact on performance. This trade-off between security and efficiency is beneficial but when the system is penetrated taking advantage of weaker cryptosystems in the course of optimization this is a vice. For these challenges, cryptographer has proposed lightweight encryption techniques and the optimization of the encryption and decryption techniques to support the optimization security requirement with little demands of the devices [45]. For example, elliptic curve cryptography (ECC) for its flexibility of offering high levels of security with less size of keys than for contemporaries.

Having reviewed the various types of threat that a PC can face, there are new and advanced types of cyber threats which include new forms of malware, ransom ware, and man-in-the-middle attacks. These emerging threats can pose a threat to cryptographic systems in very unimaginable ways. For instance, the man-in-the-middle attack can alter the contents of encrypted messages when an attacker is capable of getting access to key or when he assumes the identity of one of the transmitter-receiver pair. Malware is also used to steal of cryptographic keys or to subvert cryptographic systems meaning that even if the communication is encrypted, the message contents can be read [46]. That becomes the reason why the protection of the cryptographic systems must continually be checked and re-firmed against such threats. Cryptography of the future is to solve such problems and guarantee the inviolability, protection, and confidentiality of information. Some future directions include:

Post-Quantum Cryptography (PQC): Cryptographic systems that cannot be vulnerable to the quantum trademark are another aspect that is being developed. Another factor is continuous exploration of lattice-based, hash-based, and type II quantum-safe designs and other potential cryptosystems, which are likely to become mainstream within the next few years [47].

Block chain and Decentralized Security: The block chain and decentralize technologies are revolutionizing the way in which the security and trust is established. The future study will most probably focus on improving the block chain's efficiency and effectiveness towards its optimization and integration with other cryptographic instruments, as well as, highly private block chain [48].

Homomorphic Encryption: While researchers continue to try to improve the efficiency of homomorphic encryption its application in the fields of privacy-preserving data analysis and cloud computing may expand. Homomorphic encryption can perform arithmetic wonders on the encrypted data and computations that may be done without the need for decryption of the data [49].

Artificial Intelligence (AI) and Cryptography: The integration of AI and cryptography can create opportunities for yielding novel approaches on the most efficient way to manage keys, detect weaknesses in cipher architectures, and possibly on the design of ciphers themselves tailored to perform better in certain compute environments [50].

Quantum Key Distribution (QKD): QKD, is seen as a possible solution to the distribution of secure keys in the age of quantum computing. QMCP is based on the quantum mechanics to ensure secure distribution of cryptographic keys and continuing research in the field could lead to development of quantum-safe communication. In any case, cryptography is still one of the cornerstones of contemporary protection, although as technology progresses, it becomes increasingly questionable all the time, thus calling the branch to develop further. From quantum computing breakthrough to the shifting threat landscape, cryptographers have several factors to overcome [51]. But these are also challenges and further development of the post quantum cryptography and lightweight algorithms, and the systems for safe generation and distribution of topping keys will maintain cryptography as indispensable tool for protection of the digital world long into the future.

CRYPTOGRAPHY – ITS IMPORTANCE IN OTHER UPCOMING TECHNOLOGIES

In the constantly developing world of advanced technologies various fields are already actively adopting and implementing emergent solutions and encryption also adapts to the needs of these new fields. Nevertheless, as digital environment grows with 5G networks, IoT, block chain, and AI to mention just but these, cryptography provides the necessary means in order to safeguard data as well as individuals' privacy and secure communication. This section looks at how cryptography compliments and enables the evolutionary of such nascent technologies. The Internet of Things (IoT) is a concept that defines a rapidly expanding network of tangible objects—all ranging from consumer-level products including home appliances, garments and accessories, and wearable products to business level products like sensors and industrial machinery. IoT devices create tremendous volumes of data, much of it being personal and yet some of these IoT devices are installed in heavily secured establishments [52]. However, most connected devices are often low power, constrained devices that lack heavy computational capabilities in terms of CPU, ROM, RAM and energy reserves and thus cannot support traditional cryptographic methods.

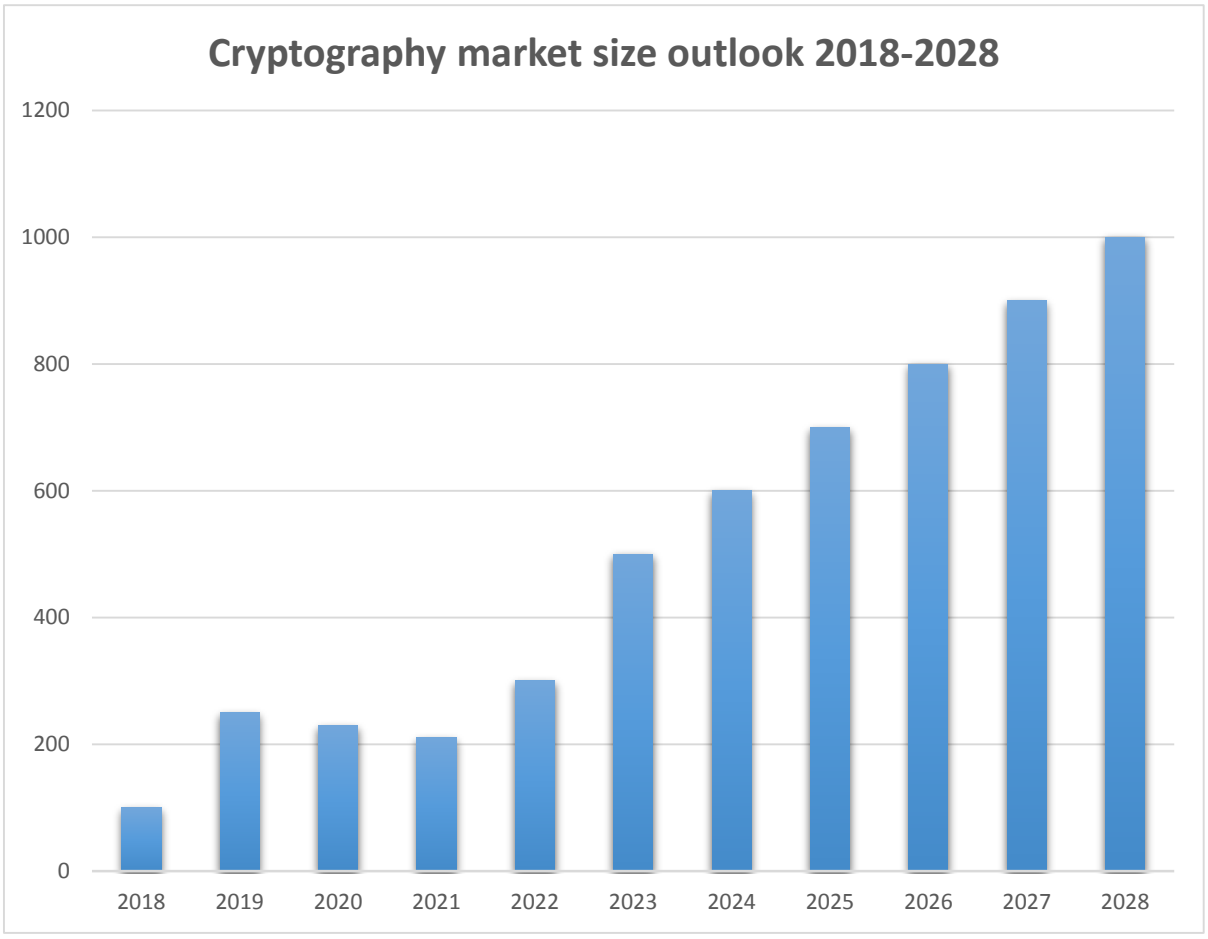

Figure: 4 showing cryptography market size

Cryptography for IoT thus has to be light, effective and can expand as the IoT grows. For example, elliptic curve cryptography (ECC) is preferred for IoT deployments because of the need to minimize the key length to have high capability encryption suitable for limited devices. Moreover TLS/SSL are employed for IoT to provide security to the device to cloud communications. Since IoT botnets and threats targeting IoT endpoints (including DDoS attacks) emerged, cryptographic security became even more essential. The sender wants to make sure that information he/she sends to the receiver stays private and this is achieved through end-to-end encryption the digital signature is used to authenticate the device of both the sender and receiver as well as to ensure that the information has not been modified en-route.

Crypto currencies such as Bit coin, Ethereum, among others use block chain technology that has strong base on cryptographic governance. It iron out the details that public key cryptography makes the digital wallets secure, while the hash functions ensure that the block chain remains to be pure, in that it produces a unique fingerprint for the blocks of data. Second, electronic signatures also qualify the genuineness of transactions, whereby only the owner of the wallet is authorized to sign for the transactions. Applications based on block chain are not just about the crypto currencies. It is also being deployed in the fields like supply chain, contracts, decentralized finance, and identity. In such uses, cryptographic methods remain pivotal for the openness, security, and fidgetiness of the dispersed structures that block chain supports [53].

Another issue that raises questions on block chain security is the issue to do with protecting the private keys. In fact, if the private key is somehow compromised then the particular digital wallet associated with it can be cleaned. This type of risk is addressed using cryptographic technologies including multi-signature wallets, threshold cryptography, and hardware security modules (HSMs) to effect secure storage and usage of the private keys. Introducing 5G networks gains unimaginable speed, bandwidth, and ultra-low latency rates; however, it comes with the risks of many securities. In particular, since 5G is intended to connect many different types of devices and applications such as autonomous vehicle, smart city, industrial automation, and more, the security of the communication between billions of devices becomes much more challenging [54].

Integrated various cryptographic technique works most vital role and is in wide use to make 5G secure i.e. data secure. The implication for security of information in transit and information in devices and nodes mean usage of encryption while the latter correspond to spying as well as altering of communications in between devices and nodes. Moreover, to make some devices authentic, and to ensure the correctness of the used software on the network equipment, public key infrastructure or PKI is used [55]. There are other areas where cryptography is applied concerning 5G, and one of them is network slicing, which is the method used to partition the network into several isolated slices to meet the specific needs as low end-to-end latency required for self-driving cars. Every slice has to be secure and cryptographic means provide that a single slice cannot make access to another one traffic, thereby promoting privacy and integrity.

As deepening the artificial intelligence (AI) technology, new topics and development opportunities also occur in the application of cryptography. There are other Apps that can also be put under artificial intelligence for example in the security where a system would be able to discern high traffic as that of an upcoming attack. However, anew with the use, or more specifically the inclusion of AI in the cybersecurity domain also poses questions on privacy and where AI systems if needs to analyze private data to train the AI equipment such as the machine learning algorithms. There is another way, in which cryptography and AI has begun to engage with one and other in the architecture of an individual's privacy preserving machine learning. For example, homomorphic encryption inherent the model that requires information could be trained on the encrypted information without decrypting it to meet the functionalities or else violate the policy of data privacy regulation. This could be more beneficial, especially in areas that Analysis data like the data of the patients in a hospital…as much as the data is sensitive, it should still be used for analysis [56].

Security of any new technologies such as IoT, block chain, 5G, AI and the quantum of computing is based on cryptography. As the delivery of routine services becomes more dependent on such technologies, cryptography has to keep responding to new threats. Predicts for the future of cryptography with relevance to EM Technology include the development of new algorithms for use in the growing volumes of data that the technologies as expected to produce in future, with regard to new types of invasions, and the unique needs of these technologies. Despite advancement in technologies three basic application of cryptography which include confidentiality, secure communication and accuracy of identity will always remain relevant.

CONCLUSION

Cryptography is the starting point for nearly all of the present day protective and security mechanisms for data, privacy, and communication. Let us discuss a brief overview of some of these cryptographic techniques: Symmetric and Asymmetric Key Cryptography: These were illustrated earlier in this text as traditional encryption methods which were formerly used prior to the advancement into the modern century cryptography Homomorphic encryption : As the name suggests it is homomorphic means same form hence the encryption form has same form of decryption form Post quantum cryptography : As known from the discussion done in this paper the quantum computing is much of threat to most of the modern cryptographic schemes hence However, the field has many challenges and these are varieties as with new industries such as; quantum computing, and the emerging and more intricate threats. Challenges against current cryptographic dominant paradigms entail new side-channel attacks, weakness due to poor key control, and growing computational power. Such threats create pressure to cryptography, since cryptography has to invent more complex protocols and employ various categories of algorithms and encryptions to defend electronic capital and information exchange data.

In future cryptography must interface with intelligent systems, block chain, IoT that will demand different form of protection. For instance, light weight cryptographic technologies are relevant for protecting the weak IoT devices; quantum for the quantum age is under development. Moreover, the AI security systems are anticipated to manage the AI/ML for detecting concerns such as the aforementioned on their own; in the same scnario, FL is anticipated to aid in gathering the ML models without compromising on the data. The constant invention of new technologies – and the rising cyber threat profiles – imply not only that cryptography must progress, but that it must extend at a quicker pace and with greater efficacy. Similar to the threat posed by quantum computing to regular encryption, the cryptographic community looks into PQ and QKD in a way that guarantees security in communication will not be threaten in future where a quantum computer can break down encryption.

It is clear that encryption is still an important factor in ensuring that confidentiality and privacy in computer based communication are assured and so must be sensitive to trends in communication technology that it seeks to protect. Its role will be most essential in guaranteeing security of autonomous systems, 5G networks and other distributed systems like block chain in the subsequent decades. Not in improving existing ones or making existing algorithms work for new purposes, but in creating new ones that would meet the current and future threats as well as find the

balance between the three aspects: security, speed, and usability are among the most frequently used essentialities that reflect website's value for the end-users. All in all, cryptography is indispensable as a stout tool for defending technologies written into our ordinary existence and prohibiting unauthorized entry into valuable knowledge.

REFERENCES

1. Bardet, Magali, Jean-Chales Faugère, and Bruno Salvy, "On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations," Proceedings of International Conference on Polynomial System Solving, 2004, pp. 71–74
2. Jao, David, and Luca De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," Proceedings of International Workshop on Post-Quantum Cryptography 2011, Lecture Notes in Computer Science, 7071, Springer, 2011, pp. 19–34.
3. Kampanakis, Panos, Douglas Stebila, Markus Friedl, Torben Hansen, and Dimitrios Sikeridis, "PostQuantum Public Key Algorithms for the Secure Shell (SSH) Protocol, Draft-KampanakisCurdle-PQ-SSH-00," Internet-Draft, Internet Engineering Task Force, 2020 (available at https://tools.ietf.org/pdf/draft-kampanakis-curdle-pq-ssh-00.pdf)
4. Kaplan, Marc, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia, "Breaking Symmetric Cryptosystems Using Quantum Period Finding," Proceedings of CRYPTO 2016, Lecture Notes in Computer Science, 9815, Springer, 2016, pp. 207–237.
5. Kipnis, Aviad, Jacques Patarin, and Louis Goubin, "Unbalanced Oil and Vinegar Signature Schemes," Proceedings of EUROCRYPT 1999, Lecture Notes in Computer Science, 1592, Springer, 1999, pp. 206–222.
6. McEliece, Robert J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory," The Deep Space Network Progress Report, DSN PR 42–44, National Aeronautics and Space Administration, pp. 114–116
7. L. J. Trautman, M. T. Hussein, L. Ngarnassi, and M. J. Molesky, Governance of the Internet of Things (loT), 60. JURIMETRICS J, 315- 51, (2020).
8. K. R. Gamache, Critical Infrastructure: Water and Wastewater Systems Sector. Encyclopedia of Security and Emergency Management, 171- 181, (2021).
9. G. N. Nguyen, N. V. Le, M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. Abd El-Latif, Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of parallel and distributed computing, 153, 150-160, (2021).
10. M. Bozdal, M. Samie, S. Aslam, and I. Jennions, Evaluation of can bus security challenges. Sensors, 20(8), 2364, (2020). [5] M. V. Rao, D. A. Reddy, A. Ampavathi, and S. Munawar, Data Mining for Cyber Physical Systems. Data Mining and Machine Learning Applications, 235-280, (2022).
11. N. L. Bhatia, V. K. Shukla, R. Punhani, and S. K. Dubey, Growing Aspects of Cyber Security in E-Commerce. In 2021 International Conference on Communication information and Computing Technology (ICCICT) (pp. 1-6). IEEE, (2021). Journal of Applied and Emerging Sciences Vol (13), Issue (01) http://dx.doi.org/10.36785/jaes.131546 7
12. C. Singh, and L. Kaur, The A REVIEW OF DIFFERENT APPROACHES FOR IMPROVING NETWORK SECURITY IN CRYPTOGRAPHY. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(1), 819-823, (2021).
13. Khraisat, and A. Alazab, A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1), 1-27, (2021).
14. Lele, Quantum Cryptography. In Quantum Technologies and Military Strategy (pp. 39-54). Springer, Cham, (2021).
15. M. Warner, J. Childress, the Use of Force for State Power: History and Future. Springer Nature, (2020).
16. L. A. Mayer, J. Schmid, S. J. Litterer, and M. S. Blumenthal, A Structured Elicitation Approach to Identify Technology Based Challenges: With Application to Inform Force Planning for Technological Surprise. RAND CORP SANTA MONICA CA, (2021).
17. D. W. Archer, T. Calderón Trilla, J. Dagit, A. Malozemoff, Y. Polyakov, K. Rohloff, G. Ryan, Ramparts: A programmer-friendly system for building homomorphic encryption applications. In Proceedings of the 7th ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography pp. 57-68, (2019).
18. T. M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez, and P. Fraga-Lamas, towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. Sensors, 19(10), 2394, (2019).

19. Hameed, M., Yang, F., Bazai, S. U., Ghafoor, M. I., Alshehri, A., Khan, I., & Jaskani, F. H. (2022). Urbanization Detection Using LiDAR-Based Remote Sensing Images of Azad Kashmir Using Novel 3D CNNs. Journal of Sensors, 2022.
20. Hameed, M., Yang, F., Bazai, S. U., Ghafoor, M. I., Alshehri, A., Khan, I., & Andualem, M. (2022). Convolutional AutoencoderBased Deep Learning Approach for Aerosol Emission Detection Using LiDAR Dataset. Journal of Sensors, 2022.
21. Feng, S., Liu, Q., Patel, A., Bazai, S. U., Jin, C. K., Kim, J. S., & Wilson, B. (2022). Automated pneumothorax triaging in chest X-rays in the New Zealand population using deep-learning algorithms. Journal of Medical Imaging and Radiation Oncology.
22. Bazai, S. U., Jang-Jaccard, J., & Wang, R. (2017, December). Anonymizing k-NN classification on MapReduce. In International Conference on Mobile Networks and Management (pp. 364-377). Springer, Cham
23. Jamil, A., ali Hameed, A., & Bazai, S. U. (2021). Land Cover Classification using Machine Learning Approaches from High Resolution Images. Journal of Applied and Emerging Sciences, 11(1), pp-108.
24. Asghar, M. N., Saleemi, F. J., Iqbal, S., Chaudhry, M. U., Yasir, M., Bazai, S. U., & Khan, M. Q. (2021). A Novel Parts of Speech (POS) Tagset for morphological, syntactic and lexical annotations of Saraiki language. Journal of Applied and Emerging Sciences, 11(1), pp-77.
25. Abbas, H., Hussain, D., Khan, G., ul Hassan, S. N., Kulsoom, I., & Hussain, S. (2021). Landslide Inventory and Landslide Susceptibility Mapping for China Pakistan Economic Corridor (CPEC)'s main route (Karakorum Highway). Journal of Applied and Emerging Sciences, 11(1), pp-18
26. Naeem, S., & Ali, A. (2022). Bees Algorithm Based Solution of NonConvex Dynamic Power Dispatch Issues in Thermal Units. Journal of Applied and Emerging Sciences, 12(1).
27. Ali, A., & Naeem, S. (2022). The Controller Parameter Optimization for Nonlinear Systems Using Particle Swarm Optimization and Genetic Algorithm. Journal of Applied and Emerging Sciences, 12(1).
28. M. Diamantaris, F. Marcantoni, S. Ioannidis, and J. Polakis, The seven deadly sins of the HTML5 WebAPI: a large-scale study on the risks of mobile sensor-based attacks. ACM Transactions on Privacy and Security (TOPS), 23(4), pp. 1-31, (2020).
29. Chesney, and D. Citron, Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753, (2019).
30. M. Elbadry, P. Milder, Y. Yang, Pub/sub in the air: A novel datacentric radio supporting robust multicast in edge environments. In 2020 IEEE/ACM Symposium on Edge Computing (SEC), IEEE, pp. 257-270, (2020).
31. D. Deebak, and F. Al-Turjman, A smart lightweight privacy preservation scheme for IoT-based UAV communication systems. Computer Communications, 162, pp. 102-117, (2020).
32. Koenig, Cacophony or Concerto?: Analyzing the Applicability of the Wiretap Act's Party Exception for Duplicate GET Requests. Fordham L. Rev., 90, pp. 951, (2021).
33. B. Al-Hayani, and H. Ilhan, Efficient cooperative image transmission in one-way multi-hop sensor network. The International Journal of Electrical Engineering & Education, 57(4), pp. 321-339, (2020).
34. Mittelbach, and M. Fischlin, the Theory of Hash Functions and Random Oracles. An Approach to Modern Cryptography, Cham: Springer Nature, (2021).
35. S. Bhattacharya, Cryptology and information security-past, present, and future role in society. International Journal on Cryptography and Information Security (IJCIS), 9(1/2), (2019).
36. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3, (2019).
37. Abu, and Z. A. Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography. International Journal of Computer Science & Network Security, 21(12), pp. 53-60, (2021).
38. M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, Encrypted control for networked systems: An illustrative introduction and current challenges. IEEE Control Systems Magazine, 41(3), 58-78, (2021).
39. C. P. Rosé, E. A. McLaughlin, R. Liu, and K. R. Koedinger, Explanatory learner models: Why machine learning (alone) is not the answer. British Journal of Educational Technology, 50(6), 2943-2958, (2019).
40. S. Perera, S.Nanayakkara, Rodrigo, S. Senaratne, and R. Weinand, Blockchain technology: Is it hype or real in the construction industry? Journal of Industrial Information Integration, 17, 100125, (2020).
41. M. Ali, A. Ismail, H. Elgohary, S. Darwish, and S. Mesbah, A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. Symmetry, 14(2), 334, (2022).

42. S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi. Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public datasmart network. Future generation computer systems, 112, 724-737, (2020).
43. D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han. Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access, 7, 54508-54521, (2019).
44. H. T. Wu, and C. W. Tsai. An intelligent agriculture network security system based on private blockchains. Journal of Communications and Networks, 21(5), 503-508, (2019).
45. C. Singh, and L. Kaur, The A REVIEW OF DIFFERENT APPROACHES FOR IMPROVING NETWORK SECURITY IN CRYPTOGRAPHY. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(1), 819-823, (2021).
46. S. Matted, G. Shankar, and B. B. Jain, Enhanced Image Security Using Stenography and Cryptography. In Computer Networks and Inventive Communication Technologies (pp. 1171-1182). Springer, Singapore, (2021).
47. J. R. Lindsay, Demystifying the quantum threat: infrastructure, institutions, and intelligence advantage. Security Studies, 29(2), 335- 361, (2020).
48. J. E. BEDI, International History of the Formative Years, Institution of Electrical Engineers, London. The Froehlich/Kent Encyclopedia of Telecommunications: Volume 18-Wireless Multiple Access Adaptive Communications Technique to Zworykin: Vladimir Kosma, 266, (2021).
49. C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), 5162, (2020).
50. H. Xu, K. Thakur, A. Kamruzzaman, and M. Ali, Applications of Cryptography in Database: A Review. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-6). IEEE, (2021).
51. Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.
52. Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *Ieee Access*, *9*, 61048-61073.
53. Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022, May). A review of quantum cybersecurity: threats, risks and opportunities. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-8). IEEE.
54. Himeur, Y., Sohail, S. S., Bensaali, F., Amira, A., & Alazab, M. (2022). Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives. *Computers & Security*, *118*, 102746.
55. Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K., Vanurin, S., & Bezzateev, S. (2020). An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends. *IEEE Access*, *8*, 103994-104015.
56. Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal*, *8*(13), 10474-10498.