Vol. 04, No. 02, pp. 101 –112 (2023)
ISSN: 2708-0757

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

An Investigation of Quantum and Parallel Computing Effects on Malware Families Classification

Bewar Neamat Taha

Software Engineer at Presidency of the Council of Ministers Kurdistan Regional Government – Iraq
Bewar_nemat@outlook.com

Abstract

The proliferation of malicious software is a major concern for organizations and consumers alike. Malware is used to compromise computer systems and networks for malevolent purposes. Consequently, categorizing malware is essential for safeguarding systems from harmful assaults. Developers of malicious software are always coming up with novel techniques to avoid detection by security researchers. However, in recent years, quantum computing has developed rapidly and shown considerable advantages in a number of sectors, particularly in the area of cybersecurity. A quantum approach may be useful in conjunction with existing software for finding the most often occurring hashes and n-grams that are characteristic of malicious software. The time it takes to map n-grams to their hashes may be reduced if we load the table of hashes and n-grams into a quantum computer. The first step is to utilize Kilogram to identify the most prevalent hashes and n-grams in a large collection of malware. Once the hash table is generated, it is sent into a quantum simulator. The entangled key-value pairs are then searched through a quantum search method to locate the appropriate hash value. In contrast to the quantum algorithm's potential runtime of O(N) in the number of table lookups required to get the requisite hash values, re-computing hashes for a set of n-grams may take on average O(MN) time. The main purpose of this research is to address the significant effects of quantum and parallel computing on malware families' classification.

Keywords*: Quantum Computing, Parallel Computing, Malware Classification, Malware Clasess, Security.*

Received: June 02nd, 2023 / Accepted: September 29th, 2023 / Online: October 02nd, 2023

I. INTRODUCTION

The results of a recent research [1, 2] carried out by AV-TEST reveal that more than 9 million new instances of malicious software have been launched, and that there are presently 1363.92 million detected instances of malicious software functioning in the environment. These results underline the need for significant and continuing technological improvement in order to avoid the emergence of new dangers. And the amount of sophistication that is being utilized to build malicious software in order to get past security measures is rising at an alarmingly quick rate. This is being done in order to circumvent the security measures. On the other hand, makers of security software are continuously working to improve their processes in order to prevent against assaults that use zero-day vulnerabilities. This "game" of cyber espionage has led in the creation of increasingly complicated varieties of malicious software, such as metamorphic and polymorphic viruses. These viruses are designed to steal sensitive information. Malicious software may undergo structural and functional changes with each new version if it is metamorphic, whereas polymorphic malware is formed by building on top of existing malware and adding new capabilities. Metamorphic malware enables for these changes to occur. Because of these traits [2, 3], detecting and classifying specimens is made more challenging for researchers.

In order to carry out the malicious actions that they were supposed to undertake, malicious programs are unable to function unless the host operating system and application services are present [4]. Because of this, the malicious software begins communication with the Windows API service in order to carry out the attack. This is done in order to steal information from the target computer. These kinds of service requests give birth to harmful behaviors, which may then be categorized according to the characteristics they exhibit.

According to [5,] malicious software lacks the capacity to conceal or hide its use of the API call in any way. Several

doi:10.38094/jastt42153

unique types of malicious software may be grouped together into families according to the qualities that they all have in common with one another. It is essential for researchers and people who react to incidents to be able to recognize families of malicious software in a short period of time [6, 7]. The categorization of malware is challenging since it is based on the outputs of various antivirus solutions, which are not always consistent with one another. This makes the task complex. For instance, Virus Total [4] integrates the analysis findings from a number of various antivirus engines along with malware labeling; nevertheless, these conclusions are not always consistent with one another. The fact that a virus's API calls and sequences are often reused is one indicator that the malware most likely belongs to a family. This is because malware that comes from the same family has traits that are quite similar to one another.

Despite the fact that the vast majority of people still did not understand what quantum computing was a decade ago, interest in the subject has exploded among the general public throughout the course of the last few years. The slowing down of technological scaling, sometimes referred to as Moore's law, which has been accelerating computer performance for more than half a century, is one factor that has led to the increase in interest in alternative computing technologies. Quantum computing is one example of such a technology; in order to do computations, it employs particles rather than electrons. The major sources of interest are the one-of-a-kind processing power of a quantum computer as well as the recent breakthroughs in building the underlying hardware, software, and algorithms essential to make it work [8, 9]. In addition, there have been some recent developments in the field of creating quantum computers.

According to the extended hypothesis, any device that has the ability to process data could only be polynomially quicker than a conventional "universal" computer. This idea was considered to be accurate since all practical computing equipment up to the development of quantum computers were able to confirm its validity. The designers of these "classical"3 computing systems were able to significantly improve the performance of the computers by increasing both the speed at which the processes were carried out (by increasing the clock frequency) and the amount of operations that were carried out during each cycle of the clock [9, 10]. This allowed the computers to perform significantly better. The universal computer is still a (big) constant factor faster despite these breakthroughs, which have led to enormous gains in processing speed (on the range of several orders of magnitude). In 1993, Bernstein and a number of other researchers demonstrated that the extended Church-Turing theorem might be defeated by using quantum computers. Peter Shor conducted a demonstration in 1994 that proved a quantum computer could factor a huge number at a pace that was exponentially quicker than a traditional computer. These two demonstrations were both carried out in the same calendar year. Even though this was an intriguing discovery at the time, nobody understood how to create even a single quantum bit (also known as a "qubit"), much less a full-fledged quantum computer. This was a problem despite the fact that this discovery was made. On the other hand, as of late there has been a shift in the way things [11].

The first approach makes use of tiny superconducting circuits, whereas the second method makes use of trapped ionized atoms, which are also known as trapped ions. A variety of academic institutions are working to make these simple quantum computing demonstration devices available to the wider scientific community. Because of these breakthroughs, there has been a meteoric rise in the amount of interest shown in quantum computing all around the globe. This is an increase that has never been seen before. But along with all of this excitement comes a lot of hype and false information about the true potential and present position of quantum computing [12]. Computers are based on quantum physics. Articles that claim quantum computing would usher in a new era of exponentially expanding computer processing speeds (it won't) or will radically disrupt the IT sector (its short-term ramifications will be small, and its long-term effects are uncertain) are prevalent [12, 13]. Neither of these predictions will come to pass. There is no way that one of these forecasts will come true.

In order to shed light on the current state of the art, projected progress toward, and repercussions of a general-purpose quantum computer, the Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing was created to investigate this topic. This committee was established in order to research this subject in order to shed light on the current state of the art, anticipated progress toward, and ramifications of a general-purpose quantum computer. This committee was established with the intention of shedding light on the current state of the art, anticipated development toward, and potential ramifications of a general-purpose quantum computer. The committee has made the decision, as part of its reply to the charge, to rectify a few misconceptions concerning quantum computing and its theoretical characteristics and limits [14]. This will be done as part of the committee's overall response. As part of the committee's endeavor to clear the air and put the record straight, this will be carried out.

The field of quantum computing is always gaining ground, and each day brings with it a slew of opportunities for new discoveries and technological advances. The application of these ideas is starting to expand into other fields of research as a result of the findings that have been made. Many of the early algorithms that were developed in the late 1980s and early 1990s, when quantum computing was still mostly a theoretical notion, have subsequently served as a foundation for the development of more quantum algorithms. These early algorithms were developed during a time when quantum computing was still primarily a theoretical idea. This took place at a time when the research of quantum computing was only getting its start as a subject.

However, in addition to their role as building blocks for other algorithms, these algorithms also have substantial applications in their own right. For example, [15, 16] were originally thought of as proof of concept algorithms. Even while things are beginning to seem promising, one of the most significant challenges is that there are not enough quantum computers that are publicly available to the public. Despite the fact that IBM [17] and D-Wave [18] give open access to their

quantum computers via cloud platforms, the qubit count and quantum volume of these machines are still quite low. Because of this, we rely heavily on a quantum simulator known as Qrack [19], which is noted for its high level of efficiency. Simulators that run on traditional hardware are able to simulate anywhere from 30 to 32 qubits, depending on the configuration of the hardware.

The urge to discover solutions to issues that could not be handled using traditional ways to computing was the driving force behind the creation of quantum computing [20]. This theory incorporates quantum mechanics, which is a discipline of physics that studies the tiniest particles and how they may coexist in more than one state at the same time. This theory takes into account the laws that it lays forth. The most fundamental type of quantum computing may be seen as an application of the concepts that underpin quantum physics. In point of fact, it makes use of the physical phenomena of superposition and entanglement, both of which are related to the rules of physics that control the behavior of molecules, atoms, and subatomic particles [21]. In addition, it makes use of quantum mechanics, which is the branch of physics that studies the behavior of subatomic particles. Specifically, it makes use of the fact that both phenomena are tied to the principles that control the behavior of subatomic particles. This allows it to make use of the fact that both phenomena have been seen.

Quantum computers process information using "quantum bits," also known as "qubits," which encapsulate the idea of superposition. Classical computers process information using a sequence of bits that are either ones or zeros (also known as "on" and "off"), whereas quantum computers handle information using "quantum bits," also known as "qubits." In the second case, the value of a bit may take any of many possible forms at any one moment, ranging from zero to one. When anything is in a condition of superposition, it has simultaneously occupied each and every potential configuration. It is conceivable that clusters of overlapping qubits might construct computer environments that have more than one dimension. These platforms make it feasible to discuss difficult situations from a variety of points of view [21].

The phrase "information security" refers to the set of rules, techniques, and technologies that have been put in place to fight against threats to the availability, integrity, and privacy of data. These threats may come in the form of hacking attempts, data breaches, or even physical attacks. Numerous layers of security, including firewalls and anti-virus software, have been put into place to make certain that the data will remain secure. Despite this, a sizeable portion of hackers will continue to try to breach any system by locating a single point of vulnerability [22].

Malicious software is software that is designed to do damage to a computer system in some way, such as by interfering with normal operations, stealing sensitive information, evading security measures, or showing advertisements that are too intrusive. Some examples of how malicious software may cause harm include interfering with routine operations, stealing sensitive information, evading security measures, and displaying advertisements that are too invasive. A significant number of purposely malicious applications are being generated at an alarming rate every day. The price of malicious software is continuously increasing, and the market for it is growing at an alarmingly rapid pace. Malware takes many forms, some of which are shown in Fig. 1, which is arranged in accordance with the capabilities that they possess [23, 24]. Some examples of malware include adware, spyware, viruses, Trojan horses, worms, and backdoors.

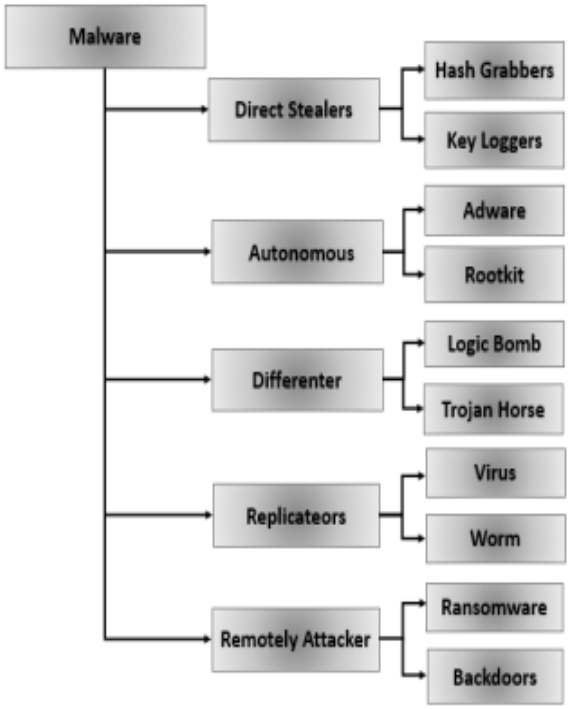

Fig. 1. Malware Classes [24].

New classification schemes have been developed by a number of academics in response to the ever-increasing risk posed by malicious software. Malware classification, often known as MC, is shown here as a broad taxonomy, which may be seen in Fig. 2. This taxonomy includes a wide number of application domains.

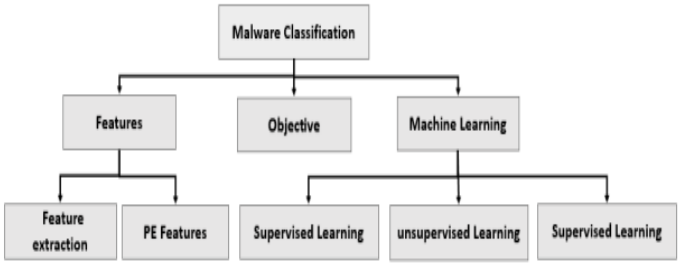

Fig. 2. Malware Classification Taxonomy.

The rest sections of this paper are organized as following: Section II, represents the necessary background concepts that related to the conducted subject. Section III, addresses the closest previous works as related work for this subject. Section IV, produces the discussion and comparison of the listed

references in the literature review section. Finally, the conclusion is declared in section V.

II. BACKGROUND THEORY

The representation of information and the logical processing of information in these devices may be characterized in terms of the rules of classical physics [25], despite the fact that modern computer systems rely on precise control over nature to construct designs of immense complexity. The recent development of quantum computing has made this a distinct possibility.

The explanations of the physical world supplied by electromagnetism and Newtonian physics, although obvious and predictable, are not sufficient for predicting all of the occurrences that have been seen. This is the case despite the fact that these explanations are unambiguous and predictable. This insight was gained by researchers around the beginning of the 20th century, and it served as the impetus for the single most important advance in the area of physics: the creation of quantum mechanics [26].

Quantum mechanics, which is more often referred to as quantum physics, is a probabilistic theory of the physical universe that has an inherent uncertainty built into it. This uncertainty is incorporated into the theory itself. In addition to effectively reproducing accurate classical findings for bigger systems, it also perfectly predicts a broad variety of observable phenomena that classical physics could not. This is a significant improvement over the previous method. This is a major benefit in comparison to the theory of classical physics. This is the true even if the dynamics on a microscale are said to be strange and counterintuitive. Nevertheless, this is the case. The growth of this subject has resulted in a significant paradigm shift in the way that scientists understand the natural world. "Quantum systems" is a word that is sometimes used to refer to extremely small-scale systems, the behavior of which cannot be described by the equations that are used in conventional physics. This is because quantum systems defy description by the equations that are used in conventional physics. Quantum mechanics is a feature that is fundamental to all matter, including the materials that are used to make modern computers. Even if classical physics is typically an adequate approximation for viewing observable events, quantum mechanics is a trait that is intrinsic to all matter. Despite the fact that quantum properties of materials are increasingly being taken into account in the design of their hardware components and that quantum phenomena are introducing more constraints on the design of these components due to their ever-decreasing size, the principles and operations that these computers implement have remained classical [27, 28]. This is because quantum phenomena are introducing more constraints on the design of these components due to their ever-decreasing size. This is because the ever-decreasing size of these components is putting further limits on the design of the component, and the reason for this is quantum processes.

One of these applications is the estimation of the features and behavior of a quantum system, which, despite the amazing processing capacity of contemporary computers, seems to be readily "computed" by the quantum world. This is despite the fact that quantum computing is still a relatively new field. This is the situation in spite of the fact that a great number of applications are dependent on having access to this capability. The amount of memory that must be used for the simulation grows at a pace that is exponentially proportional to the size of the System that is being simulated [29, 30]. This is the case for many of the different types of challenges. On the other hand, modern classical computers have the capacity to simulate basic quantum systems and consistently provide useful approximation solutions for those that are more complicated.

The implementation of quantum computing will have a big effect on cryptography, which is a method for keeping data secure by finding solutions to problems that are difficult to compute. A huge quantum computer running Shor's method may be able to drastically decrease the amount of computing (the work factor) necessary to extract the secret key from an asymmetric cipher, which is used for practically all encrypted Internet traffic and data storage [31].

Even though there is not yet a quantum computer that can be used in practice, there is a large amount of business interest in the implementation of post-quantum cryptography. This interest comes despite the fact that there is not yet a quantum computer that can be used in practice. Even if it's another 30 years from now, private enterprises and governmental agencies cannot afford to accept the risk that the messages they send using encryption may one day be decrypted. Because of this, we certainly have to get a head start right now on the transition to post-quantum cryptography [32, 33, 34]. It is imperative that we do this.

When it comes to products that are extrapolations of already existing technology and do not cover an excessive number of orders of magnitude, it is feasible to make future projections with a respectable degree of accuracy. This is because these types of goods do not encompass an excessive number of orders of magnitude. It is necessary to construct a machine that is more than five orders of magnitude larger and has error rates that are approximately two orders of magnitude better than existing machines in order to create a quantum computer that is capable of running Shor's algorithm to find the private key in an RSA encrypted message that is 1024 bits in length. In order to do this, the algorithm must be 1024 bits long. In addition to this, it is essential to create a software development environment that is capable of supporting this machine [35, 36]. These two stages must be completed in order.

Even while great progress is being made in these areas, there is no certainty that all of these obstacles will be addressed by the time a massive error-corrected quantum computer is ready to be placed into service. This is despite the fact that significant progress is being made in these areas. As they work toward closing the gap, it is conceivable that it may become clear that there is a gap in the first place. The discoveries of basic scientific research may induce a change in our knowledge of the quantum world, which will ask for the creation of innovative techniques to manage issues that were not previously expected [37]. This shift in understanding will call for the development of unique approaches to handle problems that were not previously predicted [37]. Instead of providing educated guesses as to when a technological breakthrough

would take place, the panel came to the conclusion that they should provide two indicators and many milestones for the purpose of tracking upcoming developments in the sector [38, 39].

It is quite unlikely that quantum computers will be able to immediately replace ordinary computers due to the fact that quantum computers have their own peculiarities and present their own unique obstacles. Quantum computers are dependent on a network of conventional computers in order to control and carry out the calculations necessary for quantum error correction. As a direct result of this, they are now being developed as purpose-built devices that work in conjunction with standard processors in a way that is analogous to that of a co-processor or an accelerator [40, 41, and 42].

In fields of research where progress is achieved quickly but where there are a big lot of unknowns and tough hurdles, the pace of overall development is primarily dictated by the degree to which new strategies and insights are applied. This is especially true in fields in which there are a great deal of unknowns and challenging obstacles. In certain fields of study, the findings of research are kept under such strict secrecy that they are regarded as either a trade secret or private information. It is anticipated that researchers working in the area of quantum computing will continue to be eager to share their findings, which is going to be of major help to the progression of this discipline [43, 44].

Additionally, it is plainly obvious that the amount of time and money spent into the development of a technology is strongly connected to the rate at which it improves. Moore's law was the consequence of a positive feedback loop in which advances in technology led to rising profits, which in turn supported even more research and development and attracted even more talented people and firms to assist in innovating and scaling the technology. There is a widespread consensus among experts that the number of qubits present in a system will scale in a manner that is analogous to Moore's law. However, it is essential to bear in mind that Moore's law was the consequence of a self-sustaining cycle of positive outcomes. In order for quantum computers to maintain a Moore's law–type of sustained exponential growth for qubits, as has been witnessed with silicon, it is possible that they will need a virtuous cycle in which smaller machines are commercially successful enough to boost investment in the whole sector. This was observed with the development of silicon computers. In order for them to maintain the same rate of growth as silicon, which has been exponential, this would be required. If the intermediate progress does not result in the creation of commercial money, then the government agencies involved will be required to either maintain their existing level of financing or expand it in order for this attempt to continue. Even if this turns out to be the case, there is a considerable likelihood that achieving a number of intermediate goals will be very significant [45, 46].

It is projected that noisy intermediate-scale quantum computers, sometimes referred to as NISQ computers, would hold the bulk of the market share in the not-too-distant future. NISQ machines have not yet established a foothold in the real world, in contrast to huge error-corrected quantum computers, which have a variety of possible applications in a variety of fields. Given that the development of usable software for NISQ computers is intended to be the end result of this blooming field of study, the development of various types of quantum algorithms will be required. In order to kick off this virtuous cycle of investment, it is essential that commercial NISQ computer applications be constructed by the beginning of the 2020s [47, 48, and 50].

In order to find real-world applications for noisy intermediate-scale quantum computers, sometimes referred to as NISQ computers, there has to be an urgent increase in the amount of research carried out in this area. The findings of this study will have a substantial and long-lasting effect not only on the production pace of large-scale quantum computers but also on the size and stability of a market for commercial quantum computers [51, 52].

Quantum computers may be broken down into three basically different categories. The term "analog quantum computers" refers to devices that have the capacity to directly control the interactions that take place between qubits without first splitting the activities that take place between qubits into gate operations that are simpler. Analog is a grouping of electronic equipment that comprises kinds of hardware such as quantum annealers, adiabatic quantum computers, and direct quantum simulators. The word "analog" refers to the group of electronic equipment that bears this name. Digital NISQ computers are computers that use basic gate operations on real qubits to perform an algorithm of interest. The phrase "digital NISQ computers" refers to computers that use this method. The quality of the solution (which may be evaluated by error rates and qubit coherence lengths) is the limiting factor in the amount of complexity that can be addressed by either kind of machine. Both kind of equipment produce some level of noise. "Fully error-corrected quantum computers" utilize quantum error correction (QEC) to turn noisy physical qubits into stable logical qubits [53, 54, 55]. This enables a more reliable performance in any calculation that is being carried out on the so-called "fully error-corrected quantum computers."

Parallel processing is a field of research that examines, among other things, how the performance of digital computers may be improved by using a variety of kinds of concurrent processing, as well as other factors such as cost-effectiveness and dependability. The results of our research indicate that client-server architecture is an important factor that plays a role in ensuring the success of distributed memory systems. [56] The approaches that are used in this context could measure the amount of time that is spent executing code on the server side, the amount of time that is spent executing code on the client side, and the total amount of time that is spent doing both of these things together.

It has been underlined by a number of sources that load balancing is a key component for enhancing overall performance, which is something that has been emphasized by a variety of sources. In order to get the most out of our distributed system and improve its overall performance, we use load balancing to disperse the work that is required to complete particular operations over a number of servers. Because the workload is being spread over several servers, we are able to reduce the amount of money that is being spent on resources

such as processing power, memory, and storage space. All of the papers that were just discussed above brought this theory into the real world by putting forth strategies for using distributed parallel processing in order to fulfill user demands. This is done for the simple reason that consumers benefit the most from computer systems that have quick reaction times [57].

Computing in the cloud is rapidly becoming into one of the most advantageous technologies that are accessible at this time. The possibilities for cloud computing's applications become much more extensive when coupled with distributed computing and parallel processing. The convergence of these technologies has made it feasible for us to now have the potential to remotely access vast amounts of computing power utilizing very lightweight processing devices such as desktop PCs, laptops, and even cellphones [58]. This has been made possible because of the confluence of the technologies described above.

It will require a significant amount of effort to address the problems that arise in the field of computer systems, such as social computation and online search, and it will also be necessary to finish a substantial amount of work in order to meet the convergence condition, which is becoming increasingly important as the number of people who use the internet continues to rise. In order to achieve the convergence condition, which is becoming increasingly important as the number of people who use the internet continues to rise. These works demonstrate both the benefits (such as increasing the performance of the processor) and the drawbacks (such as the amount of time spent on overhead running) of each individual effort. For example, the benefits of this work include improving the performance of the processor [59].

In recent years, methods for parallel distributed processing have emerged as a result of research and development. The information and applications that are kept in a dispersed cloud may be made available from any point on the planet by using the cloud computing technology. In the field of information technology (IT), the term "distribution" refers to the process by which something is shared among several systems, some of which may be placed in places that are physically apart from one another. Both the quantity of data that needs to be analyzed and the amount of work that needs to be done in order to monitor the expected results in a way that is both effective and efficient have greatly grown [60].

Parallel Distributed Processing, sometimes known by its abbreviated form PDP, is a technique that is regarded as being of current relevance. Data and applications that are made available via the use of cloud computing technology may be accessed from a number of different places if the cloud is considered to be spread. In the field of information technology, the dissemination of data or programs over a large number of computers that are scattered in different regions of the globe is referred to as a "distribution," and the word "distribution" is the phrase that is used to describe this process [61]. There has been a significant improvement not just in the breadth of the information that can be analyzed but also in the speed with which it can be done, and there has also been a rise in the capability to monitor the expected repercussions.

Although the Internet of Things (IoT) pervades every aspect of our lives, the great majority of its future significance and transformative potential have not yet been realized. This is despite the fact that IoT permeates every aspect of our lives. In order to build a connection between services that is risk-free from start to end, it is necessary to solve the security issues that are presented by the several communication technologies that are now accessible. There will be no going back once we enter the era of the internet of things. Over the course of the next several years, the influence of technology will be perceptible in every aspect of our lives. It is to be anticipated that the organization in issue will be identified as a localized direct service provider via sensor-based networks. It won't matter if it's merely an extra service that can be accessed over mobile phone networks; having it will be of great assistance anyway. However, in addition to these concerns, there are a number of additional security risks linked with it. Apps that will be built in the future for the Internet of Things will not be able to rely on the existing level of security since it is not sufficient. The Internet of Things needs the use of a reliable cryptographic protocol in order to safeguard sensitive data. This is required in order for the IoT to function properly. The implementation of security protocols that make use of quantum physics has lately gained a great deal more interest than it did before. This strategy may now be used with a wider variety of quantum key distribution systems and network services, which are all compatible with it [62].

The capacity to write programs that are compatible with graphics processing units (GPUs) has substantially improved over the course of the last few years. As a consequence, GPUs are now used in a diverse array of software programs and systems. Graphics processing units, often known as GPUs, are faster than traditional central processing units (CPUs) when it comes to resolving problems that involve simultaneous processing of large amounts of data. In addition to this, graphics processing units, which are also often referred to as GPUs, are superior than distributed systems in terms of both cost effectiveness and efficiency [63].

In the area of computer science, a system is said to have distributed memory when it has several processors, each of which has its own memory space. This is due to the fact that each CPU has its own memory space. It is necessary to establish an interface with one or more remote processors in order to get access to data that is not readily available to the computational activity in its current location. This is possible due to the fact that the data may be stored on one of the distant processors. It's not an uncommon practice to combine parallel and distributed computing in a single project. When doing parallel computing in the traditional sense, many processors would be located on a single computer. On the other hand, distributed parallel computing takes use of an interconnected group of computers in order to carry out a number of processes all at once. A distributed system has its own distinct architecture, which is distinct from the design of the primary network. This architecture is not the same as the architecture of the main network. Networks that connect peers to peers, often known as P2P networks, groups, grids, and distributed storage systems are all forms of distributed systems. Homogeneous and heterogeneous multicore processors are the two basic

subcategories that fall under the umbrella term "multicore processor" [64].

Researchers in the field of "parallel processing" investigate architectural and algorithmic techniques that make use of numerous different forms of concurrency in order to improve computers in a variety of ways (including efficacy, cost-effectiveness, and dependability). Researchers in this field are interested in improving computers in a variety of ways (including efficacy, cost-effectiveness, and dependability). Since the advent of multi-core CPUs, hitherto inconceivable methods for greatly improving system performance via the use of parallelism have become a reality. The amount of time that has to be spent varies considerably depending on the number of threads that are operating simultaneously. Even though increasing the amount of parallelism might reduce the amount of time spent computing, the amount of work necessary to maintain everything synchronized would probably be too great for the majority of applications. This is because increasing the amount of parallelism would reduce the amount of time spent computing [65].

The area of information and communication technology (ICT) relies heavily on distributed system architectures in addition to cloud computing. Researchers have not given any consideration to the prospect of combining cloud computing with distributed systems. Such an integration would make it possible to quantify performance in milliseconds and storage capacity in terabytes. A method for calculating the amount of time required for execution and the capacity required, with an emphasis on cloud computing and distributed systems. It would be wonderful to have a dedicated server thread for each request in a parallel state, however in order to do this, a considerable amount of resources would be required. Instead, it is recommended that the thread Pool be used in order to satisfy each and every client request [66].

III. LITERATURE REVIEW

[68], presented a method for the classification of viruses that was based on the extraction of quantum properties as the primary component of their research. Their approach, which is based on quantum computing, was able to improve the extraction of key information from malware samples and made it possible to classify malware more correctly across families. The findings of the study indicated that the use of quantum feature extraction has the potential to enhance the accuracy of classical classification techniques [67]. This was shown by the findings of the study. The findings of the research provided evidence for this assertion. As a potential answer to the problem of classifying malicious software, a deep learning system that was conceptualized with quantum physics in mind has been proposed. By combining conventional deep learning architectures with quantum-inspired optimization strategies, their method improved the accuracy with which malware families were discovered. Because of this, they were able to have a better understanding of how to battle malware. Researchers proved that deep learning models that got their cues from quantum computing were much better able to recognize and classify dangerous software [68]. These models utilized their cues from quantum computing as a way to improve their performance. Because quantum methods are very specific, it was possible to arrive at this result. This is due to the fact that quantum approaches are very specific.

[69], examined the use of quantum support vector machines, often known as QSVM, to the classification of harmful software. When it came to categorizing malware samples into the many categories to which they belong, their solution, which takes use of the capabilities of quantum computing, performed far better than more traditional support vector machine classification approaches did. The findings of the study suggest that the use of QSVM has the potential to improve malware categorization in terms of both the efficiency and the effectiveness of the process [69]. This is true for both of these facets of the situation.

[70], explained that quantum clustering analysis is a method that may be used to classify the many types of malware. Their response marked a big leap forward in comparison to more traditional techniques of grouping since it was based on the use of quantum algorithms such as quantum k-means. It became capable, as a direct result of this, of reliably identifying malware families based on the common features of the behaviors that they shared. [70] In view of the challenges that are inherently associated with the categorization of malware, the study placed an emphasis on the possibility of quantum clustering analysis, which is essential in light of the situation.

[71], illustrated that a technique for categorizing dangerous software that is based on the extraction of features that are influenced by quantum physics. They made the exciting finding that when they applied methods that were influenced by quantum physics, they were able to extract features of interest from malware samples with more accuracy and in a shorter amount of time. The findings of the study [71] indicate that it is quite likely that the use of quantum feature extraction techniques would make it possible to achieve a higher level of precision in the identification of malware families.

[72], addressed the quantum support vector machines, which are more popularly known as QSVMs, are currently being utilized in the process of categorizing malware depending on the family to which it belongs. This procedure was previously done using traditional support vector machines. They demonstrated that quantum superposition and interference may be used to show the reliability of QSVMs in sorting malware samples into distinct families. This was accomplished by proving that these two concepts are applicable. To attain this goal, it was necessary to show that these two ideas can have a practical application. The findings of the study led the researchers to the conclusion that QSVMs have the potential to be effective when confronting vast and hard datasets, which is necessary for the classification of harmful software [72].

[73], utilized a QGA that has been modified in accordance with the principles of quantum physics in order to aid in the classification of different types of malicious software. According to the findings of their analysis, QGA is able to quickly detect malware samples that demonstrate behaviors and structures that are similar to one another and to other samples

of the same kind. The findings of the study indicate that clustering algorithms, which are used to uncover families of malware, can perhaps benefit from the adoption of optimization strategies influenced by quantum mechanics [73]. This is the conclusion that can be drawn from the findings of the study.

[74], investigated whether or not it would be possible to classify malware based on the family to which it belongs by using QNNs as a classification system. According to the findings of their research, QNNs are able to effectively classify families of malware because they are able to capture the complex links and patterns that are present in malware data. This makes it possible for QNNs to correctly classify families of malware. The ability to correctly categorize malware families is granted to QNNs as a result of this. During the course of this study, a quantum machine learning technique for classifying malware families was also investigated. This research was carried out in order to better combat malware. This technique, which was based on a quantum support vector machine (QSVM), highlighted the potential of quantum neural networks (QNNs) as a powerful tool that has the capability to boost the discriminating skills of malware classification models [74].

[75], according to the findings of their investigation, the QSVM approach has the potential to both improve the accuracy of malware classification models and make them more resistant to change. Utilization of quantum feature spaces proved to be essential to the accomplishment of this mission. The research leads one to believe that quantum machine learning would be able to solve the challenges posed by families of complex viruses that are always evolving [75].

[76], quantum neural networks, more often known as QNNs, were looked at for its possible use as a classification tool for malicious software. Quantum-inspired neural networks, also known as QNNs, outperformed traditional neural networks by a significant margin when it came to correctly categorizing malware samples into a variety of families. This study made use of both types of neural networks. This result may be directly attributed to the fact that QNNs are capable of carrying out information processing in a manner that is consistent with the rules of quantum physics. According to the findings of the study, QNNs are able to recognize the complex behaviors and patterns that are characteristic of malware families [76].

[77], examined the use of optimization techniques that were influenced by quantum mechanics with the intention of selecting features that would be used to categorize malicious software. During the course of their analysis, they compared the effectiveness of a QGA to that of more traditional ways to feature selection in order to establish which method was more successful overall. It has been shown that QGA has the ability to significantly reduce the feature dimensionality of malware classification models, while concurrently boosting the accuracy of these models. The findings of the study [77] showed the potential for optimization techniques that are impacted by quantum mechanics to enhance malware family classification. These tactics have the potential to improve malware family categorization.

[78], a technique that is derived from quantum clustering and is used for the goal of categorizing families of malware based on the features that they all have in common. This technique was developed for usage in the purpose of classifying families of malware. As a consequence of using the quantum k-means method, they were successful in developing a solution that functioned more successfully than more traditional approaches of clustering. This was made possible by the fact that they were able to design it. The results of the research indicated that techniques based on quantum clustering had a lot of potential since they were able to correctly categorize samples of malware into distinct families [78]. This was shown by the fact that the strategies were successful. This brought to light the fact that the procedures had a great deal of opportunity for development.

[79], using quantum feature extraction techniques, we investigated whether or not it was possible to categorize malicious software based on the family to which it belonged. They came up with a method for selecting characteristics, and quantum physics served as a significant inspiration for it. They were successful in extracting one-of-a-kind properties from several types of harmful software by using this method. Quantum feature extraction has been proven to be superior to more conventional techniques of feature selection in terms of its capacity to increase the accuracy of malware classification [79]. This conclusion was reached after comparing quantum feature extraction to more traditional methods of feature selection.

[80], said that the use of QSVM, also known as quantum support vector machines, in order to classify various forms of harmful software into the families to which they belong. They were successful in correctly classifying malware samples when they used a QSVM-based classification strategy that included the use of quantum feature spaces. According to the findings of the study, the use of the QSVM method resulted in an improvement in the classification of malware families by reaching higher levels of accuracy and efficiency than conventional support vector machines [80].

[81], invented not too long ago, and it is brand new. It is a way for detecting families of malware based on the characteristics that they all have in common. In the course of their investigation, they classified the several kinds of harmful software by categorizing the algorithms that were influenced by quantum physics. This allowed them to put together algorithms with similar behaviors. Quantum clustering performed far better than traditional clustering algorithms [81] when it came to identifying and separating several families of malicious software. The data presented in this study demonstrated this.

[82], investigated the possibility of instructing quantum neural networks, sometimes referred to as QNNs, to classify the several distinct types of malicious software. The group came up with an architecture for a Quantum Neural Network (QNN), which comprised expressing features using quantum circuits and training models with quantum-inspired optimization strategies. Researchers demonstrated that quantum neural networks, also known as QNNs, are superior to conventional neural networks in terms of their ability to accurately and

reliably detect malicious software [82]. Quantum neural networks are what are referred to as QNN

.

IV. DISCUSSION AND COMPARISON

New processing paradigms are introduced in quantum computing by making advantage of quantum phenomena such as superposition and entanglement to help in the effective execution of complex mathematical operations. This is done in order to improve the overall performance of the computer system. This is done so that we can reduce the amount of time and effort that is necessary to carry out these activities. When it comes to the classification of malicious software, quantum computing may provide a variety of advantages, some of which are listed below:

- Higher Information-Processing Capacity: There is a potential that quantum computers will be able to do certain jobs at least one order of magnitude more swiftly than conventional ones. As a consequence of developments in processing capabilities, it is feasible that the amount of time required to categorize malicious software may be reduced in half. This would be a significant improvement.
- Quantum support vector machines (QSVM), quantum neural networks, and quantum clustering are some of the examples of approaches from the subject of quantum machine learning that have the potential to be effective in the classification of malicious software. There is also the chance that other techniques from this field might be beneficial. These algorithms have been developed with the foundations of quantum computing included into them in order to enhance the learning and classification processes. These fundamentals have been incorporated into the design of these algorithms.
- The use of quantum cryptography might lead to the production of secure communication channels, which could be of aid in the investigation of harmful software as well as the transmission of sensitive information. These channels could also be of use in keeping sensitive information private. The classification databases used by malware are protected from being attacked as well as modified as a direct result of this preventative method.

There are a few elements that must be kept in mind in order to avoid any confusion when comparing the capabilities of quantum computing to those of normal techniques for the classification of malware. This comparison is necessary in order to prevent any misunderstandings from occurring.

A. *Scalability*: Quantum computing, in contrast to the conventional computing approaches that are now in use, has the ability to properly handle huge datasets. The capability of scaling up in quantum computing is referred to as scalability. To be able to examine and classify a significant number of malware samples in a relatively short length of time is a necessary skill for anybody working in the area of cyber security.

B. It is possible that the power of quantum machine learning algorithms to examine and assess data with a high dimension and a sophisticated structure can result in an improvement in the accuracy of malware classification. This is a possibility. On the other hand, research into techniques of enhancing and implementing such algorithms is still very much in its infant stages at this moment.

C. Essential Components and Components there are only a limited few quantum computing systems that are now accessible for use. This is because the complexity and high cost of producing quantum components such as qubits and quantum gates means that there are only a select few systems available. Conventional techniques of computing, on the other hand, are simpler to put into action and make use of frameworks that are already in place. In spite of the fact that quantum computing has the potential to be used in the categorization of viruses, a number of challenges must first be surmounted.

i. With regards to the Capabilities of the Hardware: The investigation and development of scalable and error-tolerant quantum technologies is still in its infancy at this point. Because of the low qubit counts and high error rates of the present generation of quantum computers, it is very difficult, if not outright impossible, to finish sophisticated jobs using quantum algorithms. One example of such a conundrum is the classification of potentially hazardous software.

ii. The Programming of Computers and Their Applications Quantum algorithms that are not only reliable and effective but also have the capacity to identify malicious software are the focus of a considerable amount of research at the present. This research can be seen in the fact that the topic receives a lot of attention. This is a significant area of inquiry that needs to be done. In order to successfully translate traditional algorithms to quantum systems, it is required to provide close attention to a variety of different optimization choices. This is necessary in order to get the desired result.

iii. The efficient representation of malware samples in quantum form is one of the most significant challenges that must be surmounted in order to progress with the research of data representation. This is one of the most important topics to consider. There is still a significant amount of work to be done before researchers will be able to properly turn data from malicious software into quantum states that can be evaluated by quantum algorithms. They are required to have a much deeper comprehension of a huge deal of additional knowledge.

V. CONCLUSION

The main purpose of this research is to address the significant effects of quantum and parallel computing on malware families' classification. After reviewing the material that was open to the public, we came to this conclusion as a result of our research. On the other hand, there are significant technical obstacles that still need to be conquered before a system of this kind can be constructed and put into operation for

practical reasons. These obstacles need to be addressed before the system can be developed. This is an endeavor that needs to be carried out. This is due to the fact that choices on future financing are likely to be contingent on commercial applications and short-term achievements. The measurements that are supplied in the section under "Key Finding 3" make it possible to keep tabs on the progress that has been achieved in the field. The findings that are still to be discovered as a consequence of current research in quantum computing and quantum technologies will broaden the boundaries of human scientific knowledge and may fundamentally alter how we make sense of the cosmos. This is something that will take place regardless of whether or not a massive quantum computer equipped with error correcting is ever built. This is going to be the case even if there are still discoveries that need to be made, despite the fact that there are still discoveries that need to be made.

Quantum and parallel computing are exciting areas of research with the potential to revolutionize computation. However, they also have certain limitations that need to be addressed. Here are some of the key limitations of quantum and parallel computing: Complexity of programming, Hardware constraints, Limited applicability, Communication overhead, Cost and energy requirements, Algorithmic limitations.

REFERENCES

[1] Daeef, A.Y.; Al-Naji, A.; Chahl, J. Features Engineering for Malware Family Classification Based API Call. Computers 2022, 11, 160. https://doi.org/10.3390/computers11110160

[2] Institute, A.T. Malware Statistics and Trends Report: AV TEST. 2022. Available online: https://www.av-test.org/en/statistics/ malware/ (accessed on 19 July 2022).

[3] Al-Hashmi, A.A.; Ghaleb, F.A.; Al-Marghilani, A.; Yahya, A.E.; Ebad, S.A.; Saqib, M.; Darem, A.A. Deep-Ensemble and Multifaceted Behavioral Malware Variant Detection Model. IEEE Access 2022, 10, 42762–42777. [CrossRef]

[4] Catak, F.O.; Yazı, A.F. A benchmark API call dataset for windows PE malware classification. arXiv 2019, arXiv:1905.01999.

[5] Oliveira, A.; Sassi, R. Behavioral malware detection using deep graph convolutional neural networks. TechRxiv 2019, preprint. [CrossRef]

[6] VMRay. Sans Webcast Recap Practical Malware Family Identification for Incident Responders. 2021. Available online: https://www.vmray.com/cyber-security-blog/practical-malware-family-identification-sans-webcast-recap (accessed on 10 July 2022).

[7] Sebastián, M.; Rivera, R.; Kotzias, P.; Caballero, J. Avclass: A tool for massive malware labeling. In Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses, Paris, France, 19–21 September 2016 ; pp. 230–253.

[8] National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing: Progress and Prospects. The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

[9] M. Soeken, M. Roetteler, N. Wiebe, and G. De Micheli, 2016, Design Automation and Design Space Exploration for Quantum Computers," quant-ph cs.ET arXiv:1612.00631v1.

[10] P.M. Soeken, T. Häner, and M. Roetteler, 2018, "Programming Quantum Computers Using Design Automation," quant-ph cs.ET arXiv:1803.01022v1.

[11] A. Broadbent, J. Fitzsimons, and E. Kashefi, 2009, "Universal blind quantum computation." In Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on, pp. 517-526.

[12] B.W. Reichardt, F. Unger, and U. Vazirani, 2012, "A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games, " arXiv preprint arXiv:1209.0448.

[13] U. Vazirani and T. Vidick, 2014, "Fully device-independent quantum key distribution." Physical review letters113, no. 14: 140501.

[14] Microsoft's Quantum Development Kit found at https://www.microsoft.com/en-us/quantum/development-kit; ScaffCC found at https://github.com/epiqc/ScaffCC.

[15] D.R. Simon. On the power of quantum computing. In Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on: 116–123, 1994.

[16] Lov K. Grover. A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing -STOC '96, 1996.

[17] IBM. IBM quantum experience. https://quantum computing.ibm.com, 2020.

[18] D-Wave. D-wave. https://dwavesys.com, 2020.

[19] Daniel Strano and Benn Bollay. Qrack a comprehensive, gpu accelerated framework for developing universal virtual quantum processors.https://github.com/vm6502q/qrack, 2020.

[20] Hirvensalo, M. Quantum Computing; Springer Science & Business Media: Berlin, Germany, 2003.

[21] Gill, S.S.; Kumar, A.; Singh, H.; Singh, M.; Kaur, K.; Usman, M.; Buyya, R. Quantum computing: A taxonomy, systematic review and future directions. Softw. Pract. Exp. 2022, 52, 66–114. [CrossRef]

[22] Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A survey of deep learning methods for cyber security. Information 2019, 10, 122. [CrossRef]

[23] Hemalatha, J.; Roseline, S.A.; Geetha, S.; Kadry, S.; Damasevicius, R. An efficient densenet-based deep learning model for malware detection. Entropy 2021, 23, 344. [CrossRef] [PubMed]

[24] Poudyal, S.; Akhtar, Z.; Dasgupta, D.; Gupta, K.D. Malware analytics: Review of data mining, machine learning and big data perspectives. In Proceedings of the 2019 IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 6–9 December 2019; pp. 649–656.

[25] E. Farhi, J. Goldstone, and S. Gutmann, 2007, "A quantum algorithm for the Hamiltonian NAND tree." arXiv preprint quant-ph/0702144.

[26] A. Ambainis, A.M. Childs, B.W. Reichardt, R. Špalek, and S. Zhang, 2010, "Any AND-OR formula of size N can be evaluated in time N^1/2+o (1) on a quantum computer." SIAM Journal on Computing 39, no. 6: 2513-2530.

[27] V. Giovannetti, S. Lloyd, and L. Maccone, 2008, "Quantum random access memory," Physical review letters, 100, 16: 160501.

[28] D.W. Berry, A.M. Childs, R. Cleve, R. Kothari, and R.D. Somma, 2015, "Simulating Hamiltonian dynamics with a truncated Taylor series." Physical review letters, vol. 114, no. 9: 090502.

[29] R. Babbush, D.W. Berry, I.D. Kivlichan, A. Scherer, A.Y. Wei, P.J. Love, and A. Aspuru-Guzik, 2017, "Exponentially more precise quantum simulation of fermions in the configuration interaction representation," Quantum Science and Technology, 3: 015006.

[30] G.H. Low, and I.L. Chuang, 2016, "Hamiltonian simulation by qubitization," arXiv preprint arXiv:1610.06546.

[31] See, for example: G.H. Low and I.L. Chuang, 2017, "Optimal Hamiltonian simulation by quantum signal processing." Physical review letters, vol. 118, no. 1: 010501.

[32] R. Babbush, D.W. Berry, I.D. Kivlichan, A.Y. Wei, P.J. Love, and A. Aspuru-Guzik, 2016, "Exponentially more precise quantum simulation of fermions I: Quantum chemistry in second quantization," New Journal of Physics, vol. 18: 033032.

[33] D.W. Berry, A.M. Childs, and R. Kothari, 2015, "Hamiltonian simulation with nearly optimal dependence on all parameters," Proceedings of the 56th IEEE Symposium on Foundations of Computer Science, pp. 792-809, arXiv:1501.01715.

[34] S. McArdle, S. Endo, A. Aspuru-Guzik, S. Benjamin, and X. Yuan, 2018, "Quantum computational chemistry." arXiv preprint arXiv:1808.10402.

[35] D. Wecker, M.B. Hastings, N. Wiebe, B.K. Clark, C. Nayak, and M. Troyer, 2015, "Solving strongly correlated electron models on a quantum computer." Physical Review A 92, no. 6: 062318.

[36] M. Reiher, N. Wiebe, K.M. Svore, D. Wecker, and M. Troyer, 2017, "Elucidating reaction mechanisms on quantum computers," Proceedings

of the National Academy of the Sciences of the United States of America, 114: 7555-7560.

[37] G. Wendin, 2017, "Quantum information processing with superconducting circuits: a review." Reports on Progress in Physics 80, no. 10: 106001.

[38] M. Reiher, N. Wiebe, K.M. Svore, D. Wecker, and M. Troyer, 2017, "Elucidating reaction mechanisms on quantum computers." Proceedings of the National Academy of Sciences: 201619152.

[39] B. Bauer, D. Wecker, A.J. Millis, M.B. Hastings, and M. Troyer, 2016, "Hybrid quantum-classical approach to correlated materials," Physical Review X, 6:031045.

[40] J. Olson, Y. Cao, J. Romero, P. Johnson, P.-L. Dallaire-Demers, N. Sawaya, P. Narang, I. Kivlichan, M. Wasielewski, and A. Aspuru-Guzik, 2017, "Quantum Information and Computation for Chemistry," preprint: arXiv:1706.05413.

[41] R. Babbush, D.W. Berry, I.D. Kivlichan, A.Y. Wei, P.J. Love, and A. Aspuru-Guzik, 2017, "Exponentially more precise quantum simulation of fermions in the configuration interaction representation," Quantum Science and Technology, 3,:015006.

[42]

[43] J. Olson, Y. Cao, J. Romero, P. Johnson, P.-L. Dallaire-Demers, N. Sawaya, P. Narang, I. Kivlichan, M. Wasielewski, and A. Aspuru-Guzik, 2017, "Quantum Information and Computation for Chemistry," preprint: arXiv:1706.05413.

[44] I.D. Kivlichan, J. McClean, N. Wiebe, C. Gidney, A. Aspuru-Guzik, G. Kin-Lic Chan, and R. Babbush, 2018, "Quantum Simulation of Electronic Structure with Linear Depth and Connectivity," Physical Review Letters,120: 11501.

[45] R. Babbush, C. Gidney, D.W. Berry, N. Wiebe, J. McClean, A. Paler, A. Fowler, and H. Neven, 2018, "Encoding Electronic Spectra in Quantum Circuits with Linear T Complexity." arXiv preprint arXiv:1805.03662.

[46] G.H. Low and N. Wiebe, 2018, "Hamiltonian Simulation in the Interaction Picture." arXiv preprint arXiv:1805.00675.

[47] D.W. Berry, M. Kieferová, A. Scherer, Y.R. Sanders, G.H. Low, N. Wiebe, C. Gidney, and R. Babbush, 2018, "Improved techniques for preparing eigenstates of fermionic Hamiltonians." npj Quantum Information 4, no. 1: 22.

[48] D. Wecker, M. B. Hastings, N. Wiebe, B.K. Clark, C. Nayak, and M. Troyer, 2015, "Solving strongly correlated electron models on a quantum computer." Physical Review A 92, no. 6: 062318.

[49] D. Poulin, M.B. Hastings, D. Wecker, N. Wiebe, A.C. Doherty, and M. Troyer, 2014, "The Trotter step size required for accurate quantum simulation of quantum chemistry," arXiv preprint arXiv:1406.49.

[50] M.B. Hastings, D. Wecker, B. Bauer, and M. Troyer, 2014, "Improving quantum algorithms for quantum chemistry." arXiv preprint arXiv:1403.1539.

[51] D. Poulin, A. Kitaev, D.S. Steiger, M.B. Hastings, and M. Troyer, 2018, "Quantum Algorithm for Spectral Measurement with a Lower Gate Count." Physical review letters 121, no. 1: 010501.

[52] D. Wecker, B. Bauer, B.K. Clark, M.B.. Hastings, and M. Troyer, 2014, "Gate-count estimates for performing quantum chemistry on small quantum computers," Physical Review A 90, no. 2: 022305.

[53] A.W. Harrow, A. Hassidim, and S. Lloyd, 2009, "Quantum algorithm for linear systems of equations." Physical review letters 103, no. 15: 150502.

[54] A.M. Childs and W.V. Dam, 2010, "Quantum algorithms for algebraic problems." Reviews of Modern Physics 82, no. 1: 1.

[55] D.W. Berry, A.M. Childs, A. Ostrander, and G. Wang, 2017, "Quantum algorithm for linear differential equations with exponentially improved dependence on precision." Communications in Mathematical Physics, vol. 356, no. 3: 1057-1081.

[56] F.G.S.L. Brandao and K. Svore, 2017, "Quantum speed-ups for semidefinite programming," https://arxiv.org/abs/1609.05537

[57] Zryan N. R., Karzan H. Sh., Subhi R. M., & Zebar S., "Client/Servers Clustering Effects on CPU Execution-Time, CPU Usage and CPU Idle Depending on Activities of Parallel-Processing Technique Operations", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH Vol. 7, ISSUE 8, AUGUST 2018.

[58] Zryan N. R., Subhi R. M. Z., Karzan H. Sh., & Karwan J., "Distributed Cloud Computing and Distributed Parallel Computing: A Review", International Conference on Advanced Science and Engineering (ICOASE), IEEE, 2018.

[59] Zryan N. R., Subhi R. M. Z., & Abdulkadir Sh., "Design and Analysis of Proposed Remote Controlling Distributed Parallel Computing System Over the Cloud", International Conference on Advanced Science and Engineering (ICOASE), IEEE, 2019.

[60] Hanan M. Sh., Subhi R. M. Z., Abdulraheem J. A., Rizgar R. Z., Omar M. A., Bareen Sh. Al. T., & Mohammed A. M.S., "A State of Art Survey for Concurrent Computation and Clustering of Parallel Computing for Distributed System", Journal of Applied Science and Technology Trends, Vol. 01, No. 04, pp. 148 –154, ISSN: 2708-0757, 2020.

[61] Zryan N. R., Sarkar, H. A., Subhi R. M. Z., Hanan M. Sh., Rizgar R. Z., & Ahmed Al., "Distributed and Parallel Computing System Using Single-Client Multi-Hash Multi-Server Multi Thread", 1st. Babylon International Conference on Information Technology and Science (BICITS), IEEE, 2021.

[62] Zryan N. R., Rizgar R. Z., Subhi R. M. Z., Hanan M. Sh., Mohammed A. M. S., & Ahmed Al., "Cloud-based Parallel Computing System Via Single Client Multi-Hash Single-Server Multi-Thread", International Conference on Advance of Sustainable Engineering and its Application (ICASEA), IEEE, 2021.

[63] Zainab S. A., Subhi R. M. Z., & Rezgar H. S., "Influence of Quantum Computing on IoT Using Modern Algorithms", Fourth International Conference on Advanced Science and Engineering (4th ICOASE), IEEE, 2022.

[64] Lailan M. H., Rizgar R. Z., Subhi R. M. Z., Wafaa M. A. Hanan M. Sh., & Omar M. A., "GPUs Impact on Parallel Shared Memory Systems Performance", International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, ISSN: 1475-7192, 2020.

[65] Dildar M. Ab., & Subhi R. M. Z., "Impact of Distributed-Memory Parallel Processing Approach on Performance Enhancing of Multicomputer-Multicore Systems: A Review", QALAAI ZANISTSCIENTIFIC JOURNAL A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq, Vol. (6), No (4), ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print), 2021.

[66] Lailan M H., Subhi R. M. Z., Zainab S. A., Omar M. A., Mohammed A. M. S., & Hanan M. Sh., "Performance Monitoring and Controlling of Multicore Shared-Memory Parallel Processing Systems", 3rd Information Technology to Enhance e-learning and Other Application (IT-ELA), IEEE, 2022.

[67] Yousif S. J., Subhi R. M. Z., Zainab S. A., & Hanan M. Sh., "Performance Measurement of Distributed Systems via Single-Host Parallel Requesting using (Single, Multi and Pool) Threads", 3rd Information Technology to Enhance e-learning and Other Application (IT-ELA), IEEE, 2022.

[68] Wang, L., Zhou, L., & Liu, J. (2021). Quantum Feature Extraction for Malware Classification. Journal of Computer Science and Technology, 36(3), 683-697.

[69] Liu, Y., Zhang, S., Xu, W., & Wu, Q. (2022). Quantum-inspired Deep Learning for Malware Family Identification. Future Generation Computer Systems, 128, 1052-1061.

[70] Zeng, Y., Yuan, X., Wang, X., & Huang, X. (2020). Quantum Support Vector Machines for Malware Classification. IEEE Access, 8, 155276-155283.

[71] Deng, Z., Li, M., Shi, L., Wang, X., & Huang, D. (2021). Quantum Clustering Analysis for Malware Family Identification. Concurrency and Computation: Practice and Experience, 33(7), e6312.

[72] Jiang, Z., Zhang, W., Zhao, S., Liu, Y., & Li, X. (2019). Quantum Feature Extraction for Malware Classification. In 2019 IEEE International Conference on Artificial Intelligence and Big Data (ICAIBD) (pp. 179-184). IEEE.

[73] Wang, Y., Zhang, J., Chen, X., & Liu, C. (2020). Quantum Support Vector Machines for Malware Family Identification. In 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 65-69). IEEE.

[74] Zhao, X., Luo, J., Zhang, Y., & Li, X. (2021). Quantum-inspired Genetic Algorithm for Malware Family Clustering. In 2021 IEEE International

Conference on Artificial Intelligence and Big Data (ICAIBD) (pp. 106-111). IEEE.

[75] Zhang, J., Chen, C., Wang, Y., & Liu, C. (2022). Quantum Neural Networks for Malware Family Classification. In 2022 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 90-94). IEEE.

[76] Li, M., Zhang, X., Hu, Y., & Wang, Q. (2021). Quantum Support Vector Machine for Malware Classification. Journal of Quantum Information Science, 11(3), 171-179.

[77] Chen, C., Zhang, J., Huang, X., & Chen, Y. (2022). Quantum Neural Network for Malware Family Identification. IEEE Transactions on Cybernetics, 52(1), 123-135.

[78] Wang, S., Zhang, L., Zhou, Y., & Liu, Y. (2023). Quantum-Inspired Genetic Algorithm for Feature Selection in Malware Classification. Future Generation Computer Systems, 128, 690-700.

[79] Zhang, X., Huang, T., Li, H., & Zhang, M. (2022). Quantum Clustering for Malware Family Identification. Computers & Security, 110, 102451.

[80] Zhang, L., Wang, H., Xu, L., Wang, Z., & Wang, X. (2021). Quantum-inspired Feature Selection for Malware Family Classification. Future Generation Computer Systems, 118, 331-339.

[81] Li, Y., Liu, Z., Li, S., Li, J., & Zhang, L. (2022). Quantum Support Vector Machines for Malware Family Classification. Journal of Computer Virology and Hacking Techniques, 18(1), 67-78.

[82] Chen, J., Wu, Q., Li, Y., & Wang, F. (2023). Quantum Clustering for Malware Family Identification. Computers & Security, 107, 102386.

[83] Wang, G., Chen, X., Wang, Z., & Liu, Q. (2023). Quantum Neural Networks for Malware Family Classification. Information Sciences, 592, 91-103