PROPOSED NEW SECURE HYBRID MOBILE CLOUD COMPUTING TO IMPROVE POWER AND DELAY

1 Ahmed Rahman Abdulzahra Al-Obaidi,
2 Seyed Ebrahim Dashti "corresponding author",
3 Saba Atiyah Mashaan,4 Mohammed Ahmed Kadhim Al-khafaji
1,3,4 Department of Computer Engineering, Shiraz Branch, Islamic Azad University
2 Department of Computer Engineering, Jahrom Branch, Islamic Azad University

Abstract:
Systems for large-scale distributed computing, such as cloud and mobile cloud deployments, offer wonderful services that boost both individual and institutional productivity. To meet performance requirements, cloud computing takes on the risks associated with P2P computing and introduces P2P cloud systems as an add-on to the federated cloud. These cloud deployments can handle resource provisioning at a very cheap cost because of their decentralized architecture, which is built on independent nodes and resources without any specific central control and monitoring. As a result, many mobile apps and services are prepared to easily scale to a massive user base. Among them, data-driven apps have proven to be the most popular and profitable. However, data-rich applications present additional challenges, such as storage, big data processing, and the critically important responsibility of preserving private or sensitive data. In this article, we first survey existing multi-tiered cloud architectures and then propose a method for dealing with large amounts of data. Second, we investigate P2P Cloud Systems (P2PCS) for processing and analyzing large datasets. Third, using healthcare systems as a case study, we propose a hybrid mobile cloud computing approach based on the cloudlets notion. The model is then tested in a simulated environment using the Mobile Cloud Computing Simulator (MCCSIM). The experimental result shows power and delay improve by 75% in a proposed cloud model. Finally, we strengthen our suggestions by outlining and discussing potential security and privacy countermeasures.
Keywords: Cloud, Mobile cloud computing, Big data, Data-intensive application, P2P.

1-Introduction:

The mobile cloud computing paradigm is made possible by the convergence of cloud and mobile computing, which leads to the development of useful apps and services that boost both individual and institutional productivity (Liu et al., 2015) (Manal et al.,2023). As the number of people using mobile devices continues to rise, a slew of new services and applications have emerged across a variety of sectors (including social media, academia, healthcare, and government) with the potential to generate massive amounts of information. The storage and processing of large amounts of data, user privacy, and the security of sensitive information are all issues that have been brought to light by these technical advancements (Yaqoob et al., 2016).

Massive amounts of information are collected from various sources, including cell phones, computers, traffic cameras, and sensors, and can be either structured, semi-structured, or unstructured (Oussous, 2018). In this context, "big" refers not only to the massive amount of data (often measured in terabytes, petabytes, or zettabytes) but also to the variety of data kinds and the speed at which new data is generated or acquired. Depending on the task at hand, big data

processing can be started either on demand or in cycles. Examining and analyzing large data sets to conclude is a common goal of this processing, which goes by various names.

Big data analytics can be applied to a wide variety of problems encountered in the real world. For instance, to replace and maintain machinery and equipment in manufacturing lines promptly, it is necessary to continuously monitor and analyze their performance (often every minute or even at shorter time intervals) (Wang et al., 2018). This is a real-world challenge since it requires the analysis of huge amounts of data in near-real time, collected from thousands of pieces of equipment with multiple functions. The costs to a manufacturer of not seeing a broken piece of machinery in time are high because the production line must be stopped.

Hospitals also have enormous databases containing patient information. There are several legal and ethical requirements for how hospitals handle their patients' medical records (Kurdi, 2015). This information should be easily accessible if any analysis is required to back up a medical decision. Both the decision to proceed with a procedure and the decision to either discharge or readmit a patient fall under this category. These choices not only improve the patient's health but also lower the expense of healthcare (by avoiding things like prolonged hospital stays).

However, governments likely have the largest data collection to manage to serve their constituents at the national, state, and local levels. Another example is the growing influence of social media, which is altering traditional business practices across industries such as marketing, advertising, manufacturing, and more. Another example is sports teams, who must deal with massive fan statistics to assess team strategies and forecast ticket sales. Due to their massive user bases, social media platforms must handle enormous amounts of data to better serve their customers and the businesses who advertise to them (Liu Zhong, 2023).

Cloud infrastructures are seen as a viable solution for these and other real-world issues because of their ability to process massive amounts of data promptly (Ghasemi-Falavarjani et al., 2015). Data analytics services, also known as Analytics as a Service (AaaS), are offered by most cloud providers and are an integral part of the cloud's underlying infrastructure. Analytics on large and varied datasets may be greatly aided by AaaS solutions (Ardagna et al., 2017). The cloud can be used for a variety of purposes, including gathering data of various types from reliable sources and sorting it based on relevance. Once the analysis is complete, the results can be represented to provide the insightful data that was sought and delivered back. In addition to meeting the needs of multinational corporations, the cloud provides the essential management and control capabilities necessitated by (regulatory) governance regulations (Oussous, 2018).

Peer-to-peer (P2P), federated, and centralized cloud architectures are the three most common types.

As stated by Ferrer et al. (2019), centralized architectures are employed and comprise the data centers and computing clusters of numerous cloud service providers because they are best suited for applications that demand short delays in communication. Due to the physical separation of cloud resources over vast distances, this method ties clients to the nearest data center to reduce communication latency.

Federated cloud: a method for building massive clouds by combining numerous smaller clouds (Kahanwal and Singh, 2013). When clients need to guarantee a high level of confidentiality while geographically dispersing data, a federated architecture can help. To further the federated notion, the "P2P cloud" (Kumari et al., 2018) constructs the cloud without relying on any one component for centralization or monitoring

Cloud resource provisioning is performed at a relatively cheap cost due to minimal management, and the architecture consists of autonomous peers and resources (Alberto et, 2023).
In (Fig.1), a typical P2P cloud architecture is depicted vertically. Users of a cloud service might not be aware of the underlying cloud computing platform. The level of service quality (QoS) they are getting is the sole factor that matters to them. The Service Level Agreement (SLA) for a P2P cloud should be explicit about the Quality of Service (QoS) criteria and the usage terms (Kumari et al., 2018).
In contrast, safe and dependable data storage is one of the most valuable features offered by P2P cloud systems. These cloud systems redistribute data across numerous sites, which could be in various towns or even other countries. This method has the potential to thwart hackers' efforts to steal or otherwise gain access to an exact duplicate of these files.
Data decentralization would boost performance in addition to deterring hackers by allowing relevant pieces of data to be gathered in parallel from other sites. This method of data storage may guarantee content-level protection, making it extremely difficult for unauthorized parties to access the stored data. There would be multiple copies of the same file kept, but no one would have complete control over any of them. This ensures greater data reliability.
Once data is evaluated and actionable insights are produced, the true potential of big data analytics becomes apparent. Most people agree that the most financially sound choice for big data analytics is cloud computing. The setting of cloud computing not only stores the data, but also offers users a wide range of cutting-edge machine learning, AI, and other capabilities. Users can examine and analyze data in any format, be it video, image, text, etc., using these cutting-edge methods. Traditional database approaches, however, may not be a good fit for working with such massive data sets. When multiple contributions need to be processed, database queries can become time-consuming and expensive. Data ownership and control security concerns compound these scaling constraints. Since cloud storage and access require data owners to cede control and administrative authority to cloud service providers, it poses a significant security risk.

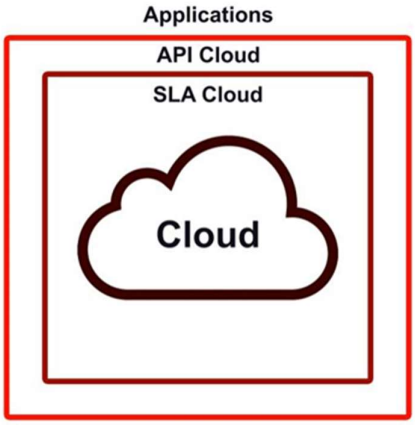

Fig.1 P2P cloud system is depicted vertically

In addition to the previously mentioned facts, there are numerous motives for conducting this research. Motivating us are the vast quantities of big data generated every second, which require efficient analysis and storage. As a real-world example, consider the medical records in the healthcare industry, where each patient has medical testing, results, X-rays, and a plethora of other data that must be processed and stored. Additionally, user data frequently contain vital

information that needs to be protected from increasingly sophisticated cyber-attacks. A recent data breach on social media networks exposed millions of private documents, to give an example from the real world. Additionally, new sophisticated hacking methods that were not available a few years ago include ransomware, spectrum assaults, and meltdown attacks, among others. Another crucial element is the demand for a secure and effective cloud/mobile cloud model to meet big data requirements.

According to the aforementioned motivations, the following can be considered to be the study's main contribution:

Examine the current tiered cloud architectures and make solid suggestions on how to store huge amounts of data efficiently in cloud-based settings.

Consider the application of P2P Cloud Systems (P2PCS) to big data analytics.

Investigate cloud and mobile cloud system security and privacy issues. We research appropriate countermeasures and suitable assaults to protect these systems from such possible dangers.

Describe a hybrid mobile cloud computing architecture that is based on the idea of cloudlets.

Utilizing the Mobile Cloud Computing Simulator, simulate the suggested model to gather experimental performance data (latency and power usage).

The relevant literature is reviewed in the section that follows. Section III discusses cloud architectures, P2P cloud, and mobile cloud systems, as well as how they satisfy big data's analytical needs. The security threats to cloud systems are covered in Section IV, along with potential defenses and safeguards. We propose our cloudlet-based hybrid cloud model in Section V, and the simulation results are shown in Section VI. Conclusions and ideas for further research are offered in Section VII.

2-Related Papers

There has been a rise in interest in P2PCS (Peer to Peer Cloud Systems) recently. Cloud computing system architectures have been the subject of some research (for example, see (Wang et al., 2018) and (Balasubramanian and Karmouch, 2017)). Newer research by (Kumari et al., 2018) focuses on constructing P2P-cloud systems from dependable, low-cost cloud resources to offer a multitude of services. There are several practical uses for the mobile cloud computing concept presented in (Lo'ai et al., 2016). Data collected by various sensors (including fire and motion detectors) and Internet of Things (IoT) devices can be stored and analyzed using the proposed methodology. The data will be sent to the mobile cloud model for efficient analysis and decision-making with limited resources.

In contrast, cloud and mobile cloud systems are vulnerable to a wide variety of assaults that could jeopardize users' privacy and data integrity (Mollah et al., 2017).

Some research even combines cloud computing with specialized services aimed at different sectors. That is to say, different types of cloud computing, such as cloud computing for manufacturing or cloud computing for healthcare, are designed to provide specialized services to their respective clientele.

The researchers (Lo'ai et al., 2016) investigated the advantages of integrating mobile cloud computing in the healthcare industry and developed a mobile cloud system based on the cloudlet idea for healthcare applications. The research team (Booth et al., 2013) underlined the properties of scientific data that are common to all fields of study in the setting of big data development. Massive scale, massive, distributed operations, complexity, and precision are all common traits.

The contributors (AlDairi and Tawalbeh, 1086) classify attacks on cloud and mobile cloud computing environments and the techniques used to defend against them. Another subject they explored was cyber-attacks on smart cities and their embedded technologies. In (Gupta et al., 2015), security concerns relating to big data and mobile cloud computing were covered. The authors (Jhuria et al., 2013) talk about the issue of inadequate security in cloud settings. They studied the many current standard encryption techniques for safeguarding data in cloud storage.

3-Big Data and Cloud Computing

Here, we first provide a summary of the layered architecture of P2PCS as described in (Kurdi, 2015), and then, in subsection 3-A, we offer a big data analytical model that we believe would be a good fit for this architecture. Big data and mobile cloud computing are two related concepts that are next to be covered in section 3-B.3.1 Peer-to-Peer Clouds

The P2P Cloud System is made up of a network of interconnected computers, or "peers," all of which run the same set of instructions (software components). In the first layer, also known as the Peer Sampling Service (PSS), a straightforward gossip protocol (Jelasity et al., 2007) ensures that every node knows which of its neighbors it can communicate with. A timestamp and an identifier (such as an IP address) are stored in each local view node's neighboring node. Based on the timestamp of the first interaction between the two nodes, the neighboring nodes are brought into the local view.

To maintain a constant list size, each node decides on its own, thus neighbors regularly share and merge their local views, deleting the oldest entries. The local view's list of nodes may vary after each message, therefore it's a dynamic list. PSS is widely regarded as an effective answer for distributed systems in which each node is responsible for managing its own set of resources.

The Slicing Service (SS) is the second layer, and it ranks nodes based on user requests. When a user requests a particular number of nodes, the cloud will divide into "slices," or groups of nodes that share the user's criteria. A user, for instance, can ask for the top-performing 5% of nodes to be used in a slice.

Aggregation Service (AS) is the third tier, and it is responsible for providing cloud-wide parameters to any node that requests them without needing to consult the global cloud registry. The total number of nodes, average load, usage, etc. are all examples of cloud-wide measures that provide insight into the health and operation of the cloud as a whole. Instead of coming from one centralized source, these figures are calculated utilizing decentralized aggregation techniques. The collected information is ingested by a Monitoring Service (MS) through APIs that are built on top of AS and may be used to monitor the node states and show the network topology.

In the P2PCS, peers from the same slice are linked together via the T-Man protocol (Jelasity et al., 2009). T-Man is a gossip-based protocol that can build arbitrary overlay networks on multiple underlying topologies. T-Man protocol uses a ring overlay to connect nodes in the same slice (Fig.2). Subclouds are created using the T-Man protocol, and failing nodes are handled by removing them from the current overlay and re-linking the remaining nodes with a new overlay while maintaining the same topology.

In P2PCS's layered design, the Dispatcher is in charge of converting high-level user commands into low-level instructions for transmission to other peers. The Instance Management Application Programming Interface (IMA) is another part of P2PCS that gives users command over resource

provisioning and destruction. The Storage system in P2PCS is another component that is built independently as a distributed service. In P2PCS, authorized users' access privileges are managed via the system's authentication mechanism.

To sum up, we recommend employing P2PCS for the aforementioned cloud-based big data storage, organization, manipulation, and movement purposes. We believe that the ideal approach to managing and analyzing large amounts of data is a hybrid of peer-to-peer and cloud computing. P2P networking, on the one hand, makes it possible for participants (peers) to maintain control of their data and even share resources across clouds by facilitating the necessary decentralization. The cloud, on the other hand, offers the storage, networking, and computing resources necessary to conduct big data analytics in a parallel and highly adaptable fashion.

In (Kurdi, 2015), the storage service is given by a set of actions such as requesting data, allotting space, etc., and the storage system is implemented independently. Partitioning data into subsets based on usage is a common method for storing massive amounts of information in P2P clouds (Liroz-Gistau et al., 2013). (Fig.3) depicts the implementation of such a partitioning to efficiently store and manage large datasets. If necessary, larger divisions might be split further in time. Here, new data is allocated to an appropriate partition based on a similarity score computed over the current partitions. The amount of queries that access the data in one partition vs the other is one model that might be used to calculate a similarity score.

4-Big data in the cloud and architecture

This part begins by summarizing the layered architecture of P2PCS as it is described in Kurdi (2015). Then, in subsection 3-A, We propose an analytical big data model that we would pair with this approach. Subsection 3-B follows with a discussion of big data and mobile cloud computing.

4.1. Peer-to-Peer Clouds

The P2P Cloud System is made up of a network of interconnected computers, or "peers," all of which run the same set of instructions (software components). In the first layer, also known as the Peer Sampling Service (PSS), a straightforward gossip protocol (Jelasity et al., 2007) ensures that every node knows which of its neighbors it can communicate with. A timestamp and an identifier (such as an IP address) are stored in each local view node's neighboring node. Based on the timestamp of the first interaction between the two nodes, the neighboring nodes are brought into the local view.

To maintain a constant list size, each node decides on its own, thus neighbors regularly share and merge their local views, deleting the oldest entries. The local view's list of nodes may vary after each message, therefore it's a dynamic list. PSS is widely regarded as an effective answer for distributed systems in which each node is responsible for managing its own set of resources.

The Slicing Service (SS) is the second layer, and it ranks nodes based on user requests. When a user requests a particular number of nodes, the cloud will divide into "slices," or groups of nodes that share the user's criteria. A user, for instance, can ask for the top-performing 5% of nodes to be used in a slice.

Aggregation Service (AS) is the third tier, and it is responsible for providing cloud-wide parameters to any node that requests them without needing to consult the global cloud registry. The total number of nodes, average load, usage, etc. are all examples of cloud-wide measures

that provide insight into the health and operation of the cloud as a whole. Instead of coming from one centralized source, these figures are calculated utilizing decentralized aggregation techniques. The collected information is ingested by a Monitoring Service (MS) through APIs that are built on top of AS and may be used to monitor the node states and show the network topology.

In the P2PCS, peers from the same slice are linked together via the T-Man protocol (Jelasity et al., 2009). T-Man is a gossip-based protocol that can build arbitrary overlay networks on multiple underlying topologies. T-Man protocol uses a ring overlay to connect nodes in the same slice (Fig.2). Subclouds are created using the T-Man protocol, and failing nodes are handled by removing them from the current overlay and re-linking the remaining nodes with a new overlay while maintaining the same topology.

In P2PCS's layered design, the Dispatcher is in charge of converting high-level user commands into low-level instructions for transmission to other peers. The Instance Management Application Programming Interface (IMA) is another part of P2PCS that gives users command over resource provisioning and destruction. The Storage system in P2PCS is another component that is built independently as a distributed service. In P2PCS, authorized users' access privileges are managed via the system's authentication mechanism.

To sum up, we recommend employing P2PCS for the aforementioned cloud-based big data storage, organization, manipulation, and movement purposes. We believe that the ideal approach to managing and analyzing large amounts of data is a hybrid of peer-to-peer and cloud computing. P2P networking, on the one hand, makes it possible for participants (peers) to maintain control of their data and even share resources across clouds by facilitating the necessary decentralization. The cloud, on the other hand, offers the storage, networking, and computing resources necessary to conduct big data analytics in a parallel and highly adaptable fashion.

In (Kurdi, 2015), the storage service is given by a set of actions such as requesting data, allotting space, etc., and the storage system is implemented independently. Partitioning data into subsets based on usage is a common method for storing massive amounts of information in P2P clouds (Liroz-Gistau et al., 2013). (Fig.3) depicts the implementation of such a partitioning to efficiently store and manage large datasets. If necessary, larger divisions might be split further in time. Here, new data is allocated based on a similarity score calculated over the present partitions, to an appropriate partition. The amount of queries that access the data in one partition vs the other is one model that might be used to calculate a similarity score.

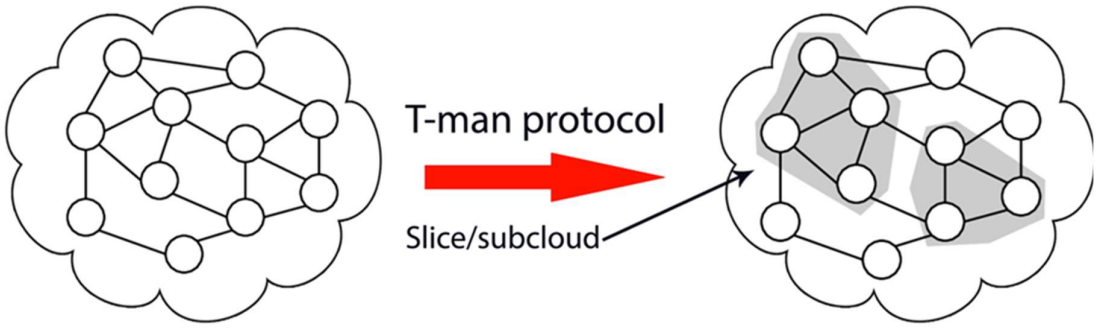

Fig.2 Creating a sub-cloud in P2PCS

4.2. Big data analytics and mobile cloud computing

Innovation in big data continues with cloud and mobile cloud computing-based advanced analytics (Fig.6). Data-driven applications continue to proliferate, simplifying a variety of tasks. The value of big data, however, is not in its sheer bulk, but in the ability to process, refine, and link massive amounts of information. For this development, also known as intelligent data, to succeed, mobile and cloud computing must work together closely (Ahmed Hadi et.,2023) (Liroz-Gistau et al., 2013). To achieve this goal, businesses will need to switch to analytical mobile applications that can filter and analyze data in real-time. Analytical programs designed specifically for mobile use are developed and hosted in the cloud.

accessed through mobile-friendly web servers; doesn't take into account device type, memory, or processing speed.

Big Data as a Service (BDaaS) is a new service that uses both Infrastructures as a Service (IaaS) and Software as a Service (SaaS) to provide analyses of complex big data via mobile cloud computing to meet the demands of organizations. Assuring security at the system and application levels is essential in this space (Gupta et al., 2015) (Manal et al.,2023).

Application security requires runtime apps that support big data analytics on mobile devices to be both self-protecting and self-aware. Therefore, the current fire barriers and perimeters cannot provide the level of security required. Developers will need to implement adaptive access control after creating such applications. On the other hand, machine learning and text mining would be coupled with other technologies at the system level to provide a variety of threat-prediction and preventive tools. Advanced protection against the perils of today's digital environment can be ensured in the future if the security problem is approached from these two perspectives.

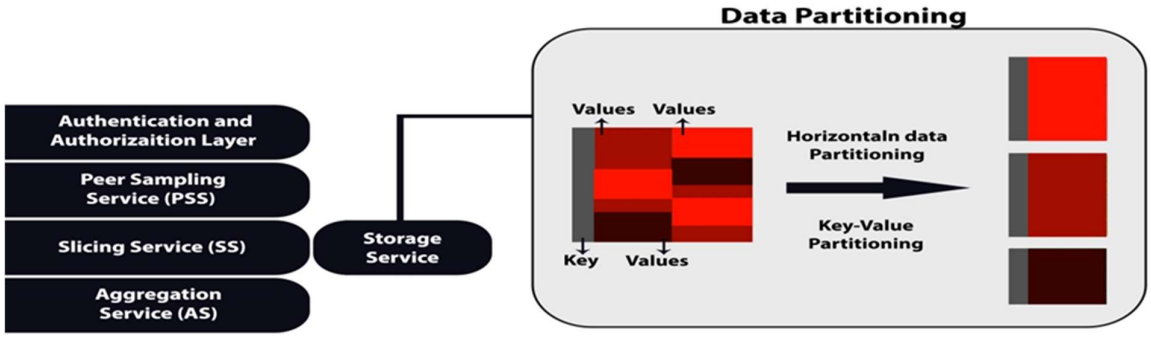

Fig.3 P2PCS storage data partitioning

4.3. Challenges

There has been a remarkable increase in the use of online monitoring of both traditional power equipment and intelligent power primary equipment (Liu, Y,2019). Keeping up with the ever-increasing volume of monitoring data presents significant technical challenges for any online monitoring system of power equipment (Javed,2017). These include the need to accommodate for "real-time," "rapid change," "high precision," "different applications," "abnormal data brought by power data," "large-scale data with complex structures," and "large dimensions." Traditional detection methods and data mining detection methods are the two broad categories into which academic inquiry may be categorized. Human experience, state estimate, the load curve, similarity, and the load change rate are the traditional foundations for power load abnormal detection approaches. As a result of its low efficiency, high subjectivity, and numerous human elements. This strategy is only effective for detecting anomalies in data when there are big, visible shifts (Rao,2022). Accelerating the detection of anomalous power load data by data

mining is artificial intelligence and cluster analysis theory, both of which are rapidly evolving. where commonly can be roughly divided into two categories: (1) the abnormal value detection method with supervised learning, which selects a portion of the power system load data as the training sample, and then uses the corresponding algorithm to ensure that the training sample and the expected output meet the corresponding requirements; (2) the detection methods based on support vector machines, artificial neural networks, and decision trees. Secondly, there is no requirement to pick a subset of the historical power load data to use as training samples when using the unsupervised learning power load abnormal data detection approach (Wang,2016). Methods like density analysis, cluster analysis, and others like them are commonly used for this purpose. One type of unsupervised method is the distance-based outlier detector. This technique yields better results when working with medium and high-dimensional data, is simple to explain, and is a representative example of a density-based outlier detection algorithm (Wang,2016). Certain parameters in the density-based abnormal load data detection approach are still dictated by subjective elements like human experience, which lowers the accuracy of abnormal data detection. Using the electric load data set's features, the abnormal value detection method based on the clustering algorithm can more correctly discriminate between normal data and abnormal data.

Medical data storage, real-time traffic monitoring, and meteorological data analysis are only a few examples of where cloud computing technology has been successful so far (Yuan,2020). Cloud computing is inexpensive and does not necessitate any special configurations or settings on the servers that make up the cluster. Integration of cloud computing's huge size and rapid calculation speed with conventional data mining approaches yields improved management and analysis of power monitoring data. With its ability to delve deeper into the shifting law of the load curve and effectively detect abnormal load data, the power load, and abnormal data detection method based on data mining and cluster analysis has become a research hotspot in recent years (Jia,2021). In practice, power load data comes in many forms, and the gap between the data's growing volume and the limitations of existing data mining methods has become increasingly obvious. There are flaws in every clustering algorithm, such as sensitivity and the inability to optimize the choice of starting parameters. That's why it's important to dig deeper into the algorithms involved in parallelizing the detection of power load data. (Fig.4) sums up the foregoing discussion (Ahmed Hadi et.,2023).

Journal of New Zealand Studies NS35 (2023), https://doi.org/ 10.5281/zenodo.7805666

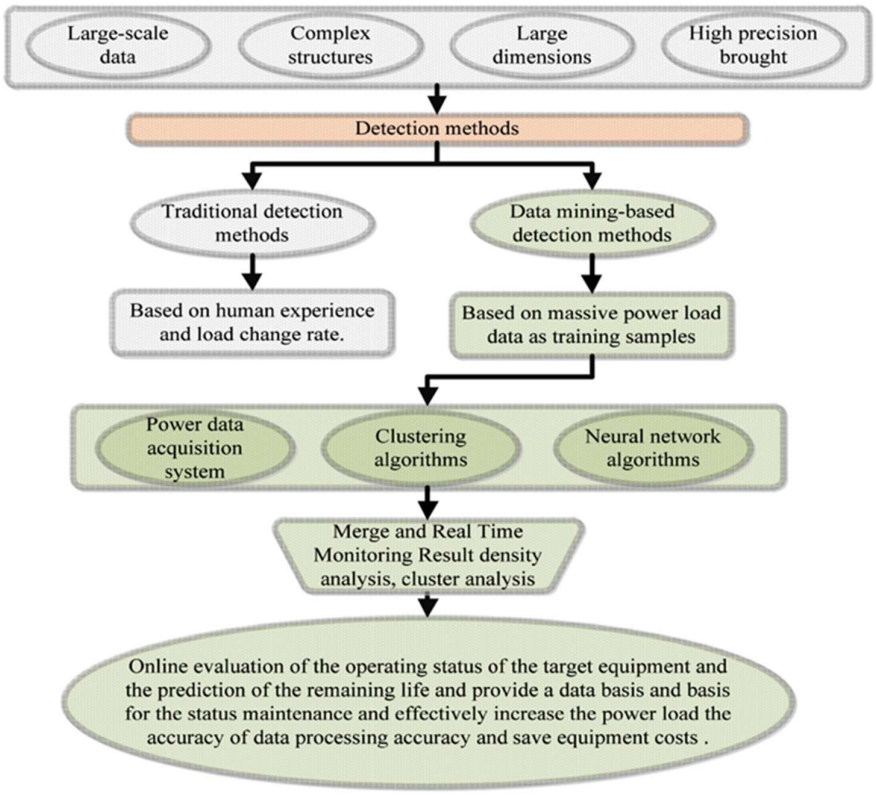

Fig.4 Power system detection methods

Research into the use of big data technologies based on cloud computing in the energy sector is still in its early stages of development. Most monitoring centers' cloud computing platforms today are built on a single Hadoop framework, which has certain limitations in terms of storing data before centralized processing, which in turn causes a processing time delay that is too great, thus failing to meet the needs of online monitoring data (Eddoujaji ,2022). Future information processing will trend towards fast and efficient data flow meetings. The most common approach involves using a database management system (DBMS), which may be incompatible with earlier systems, even though numerous research has been conducted on velocity, volume, and diversity. Real-time abnormality detection is becoming increasingly important, as is the need for fast processing of monitoring data. Though the incorporation of cloud computing into the electricity sector is a significant step forward, a more in-depth study is required before it can be used for actual power generation. The great performance of cloud computing has garnered a lot of interest, but the question of how to use it for processing massive amounts of real-time data has not been investigated (Naeem ,2019). Smart cities or digital twin cities with VR features can be built much faster thanks to multisource heterogeneous urban sensor access and data management technologies. Due to the complex operation of the integrated prediction model and meeting in real-time for intelligent power systems, the complexity of the processes has frequently grown with the single computing resources insufficient. Clustering analysis algorithms and cloud computing were developed in response to the difficulty of researching and analyzing enormous data sets related to electricity use. Cloud computing is typically implemented as a regional management framework in academic research. Consequently, there was a dearth of studies that

Journal of New Zealand Studies NS35 (2023), https://doi.org/ 10.5281/zenodo.7805666

made use of cloud computing's ability to centrally share the systems that regulate the procedure. All the research were concentrating on smart vehicles' batteries (Amir,2022), although several proposed cloud computing goods like artificial intelligence (AI) and the Internet of Things (IoT) in their models. Since it is challenging to meet the real-time requirements of the power system and build a safe, stable, cost-effective, green, and environmentally friendly smart grid, this study addresses the issue of centralized parallel processing and diagnosis of power system condition data using cloud computing and big data technology. There is a wide variety of issues related to power management and monitoring, and this work proposes to tackle three of them. Problems (Fig.5) (Ahmed Hadi et.,2023).

The inadequacy of the algorithm that combines data mining and computing technology to deal with huge data; 1. The need to meet the numerous real-time requirements of power system state monitoring; 2. The limitations of traditional data mining based on single-node serial mining; 3.

Last but not least, cloud computing has the potential to be an invaluable asset to an intelligent power system in its quest to address the problem of huge data from extensive regions. This literature review incorporates contributions that address the aforementioned concerns. In this paper, we present the first universally applicable framework for parallel optimization in power systems, which can be used by researchers to systematically describe their parallelization studies and locate them in the landscape of parallel optimization regardless of the application domain, problem addressed, methodology parallelized, or technology used. In particular, the algorithmic design and computational implementation issues of parallel optimization, which are often dealt with independently in the literature, are incorporated into the proposed strategy. Second, we use the integrative framework to synthesize previous work on parallel optimization in the realm of power systems.

Millions of intelligent meters add another layer of complexity to the task of data and information management. As can be seen in (Fig.6) and Table 1 (Ahmed Hadi et.,2023) (Shariff,2020), cloud computing may be a more cost-effective solution for data analysis and storage.

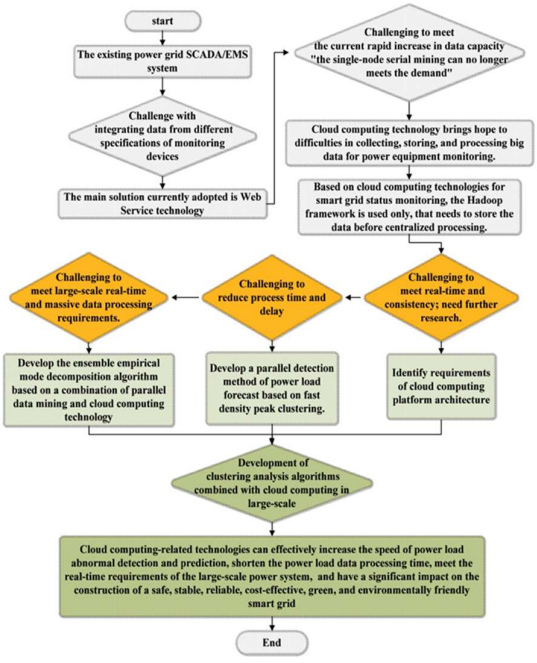

Fig.5 Overarching diagram of how the proposed system handles problems and how to fix them.

Fig.6 Cloud storage, mobile devices, and big data

Table 1: The challenges of information and data management brought on by the need to effectively handle the data from millions of intelligent meters using cloud computing

Journal of New Zealand Studies NS35 (2023), https://doi.org/ 10.5281/zenodo.7805666

Existing Challenging	Proposed Solution	Challenging Proposed Solutions and Future Work
The problem with concurrent power transmission networks is the uneven temporal distribution and the growing number of fault occurrences that cause power outages or interruptions.	The suggested model incorporates and explicitly assesses seldom occurring environmental components, faults, and periods with fewer fault events, which improves the forecast performance of power transmission fault events.	challenging to deal with the massive amount of monitoring data
The problem of conventional clustering algorithms for Big Data Analytics.	Parallel algorithms of k-means and canopy are implemented using the Hadoop environment and Mahout to solve the problem of conventional clustering algorithms.	Process locally after storage data.
Problems with traditional data mining that is generated in single-node chain mining.	This work uses single-node serial mining to tackle the classic data mining problem in power systems. It has vast storage and processing capacities, and accuracy 87%.	Did not use cloud computing so it was hard to meet real-time and large scale
The limitations of centralised administration based on LAN design prevent broad-area monitoring and the resolution it's issues.	This study describes cloud-based power grid-wide-area monitoring architecture for parallel computing and big data mining to give intelligent grid decisions.	This paper's flaw is a lack of data exchange during processing.
Considering real-time application, the smart grid still needs to advance in terms of efficiency, power management, dependability, and value.	Using cloud computing architecture from any location and at any time, design remote real-time monitoring of substation power data in a safe, efficient, and effective manner.	The weakness of this work the power flow in the grid is continuously monitored using PLC and Energy Meter, it doesn't use cloud computing applications.
Large-scale data processing and analysis methods in a real-time panoramic grid are a challenge for smart grids.	This paper use data mining and integrated information technology platform to present a smart grid building a large multi-level data storage system to extract valuable knowledge to support grid scheduling decisions.	Dealing with redundant data and noise in data mining results remains a barrier for technology. It is also uncertain if the current cloud platform will get real-time smart grid monitoring data.
As smart grids spread, terminal devices like cutting-edge sensors and smart metres tend wide access to distribution networks, providing major challenges to the information perception, analysis, and processing capacities of the distribution automation system.	This paper aims at guiding to preserve CPU and memory resources and increase resource utilisation. through presents a configuration technique for computing resources for the microservice-based edge computing apparatus in the smart distribution transformer region.	The lack is the trade-off methods between robustness and economy in computing resource configuration problems and apply the achievement of this work to investigate the computing resource scheduling problem of the cloud-edge collaborative system in the smart grids.
It has become very difficult to process big amounts of real-time data in research and applications, and it hasn't been researched how to employ cloud computing technology for large-scale real-time data processing.	This research focuses on the big data processing architecture of the cloud computing platform. It creates a large data processing calculation mode and establishes the overall real-time big data processing architecture that acts as the foundation for the RTDP (Real-Time Data Processing)	The RTDP is a tough project, and many issues still need to be researched further: Choosing the most effective technique for calculating future design performance; Real-time data processing hardware must be implemented equally.
The huge challenge of integrating and exchanging vast sensor information resources that differ widely in hardware design, connection protocols, formatting, conversational skills, sampling rate, and data accuracy.	This paper provides a deeper understanding of the needs, platforms, most current technical developments, and open research problems of urban sensor applications for academics and leaders in the IoT and smart cities sectors.	Relational databases usually struggle with scalability, availability, and concurrent reading and writing, especially for big data handling in wireless sensor networks. As IoT and sensor technology continues to progress, cloud computing will be used.

Journal of New Zealand Studies NS35 (2023), https://doi.org/ 10.5281/zenodo.7805666

The ability to detect and analyse anomalies for huge data in real-time is a tough problem due use conventional detection methods of data processing.	An anomaly detection model based on Hadoop distributed processing method, cloud computing and MapReduce monitoring framework is presented using machine learning.	The challenge to Meeting the real-time and large scale
Data from networks and smart cities is increasing and it is becoming huge so it need to big data analysis (BDA)	BDA generated in the smart city (IoT) to turn the smart city toward safety, efficient data processing, and good governance.	The flaw is the system created for the study only offers offline batch analysis and prediction functions.
Smart grids (SGs) are utilizing massive data for operations and services.	Information and communication technologies (ICTs) play an important role, particularly in the computing model, which governs how data analytics in SG may be carried out.	The design of EC systems, EC-appropriate algorithms, resource management in the EC environment, and even hardware accelerations might all be improved.
Increasing renewable energy sources making the power system more complex.	This study focuses on using ICT data in smart grid decision-making to ensure systems are secure and reliably operate.	The SCADA issues caused by ICT integration continue to exist like interdependency analysis, and decision-making.
There are challenges to controlling MGs in a logical and coordinated way	In this study, control objectives are categorized in line to the hierarchical control layers in MGs, and the development approaches given by MGSC/EMS are summarized.	the challenging issue is the uncertainty about power production related to weather, load calculation times and response time brings more challenges to MGSC/EMS.
The challenge of extracting data value through the statistical analysis of an immense amount of data generated by cyber-physical systems.	The goal of this paper was not to give the solutions, but rather to name the problems. A major challenge is the changing nature of the technical systems	software-based devices change frequently due to bug fixing and software updates. Therefore, the data we collected is after time only partially valid.
The challenge of clustering techniques in Big Data context.	Provide a thorough analysis of the Big Data clustering problems and highlight the benefits of the key methods.	Data are too big, dynamic, and complex. Traditional data handling struggle to collect, store, and analyse data.
The execution of the Hadoop cluster when processing a high number of tiny files is the true problem businesses face. The solutions are restricted to NameNode memory	Some novel strategies have been put forth, such as combining tiny heterogeneous files in various formats in a quasirandom manner, which resolves the memory issue by drastically reducing the amount of metadata.	Hadoop cannot satisfy real-time demands because it stores data before processing.
Big Data poses difficulties for Digital Earth in terms of data mining, processing, and storage. Transforming big data's volume, velocity, and diversity into values is the main challenge.	Cloud computing provides fundamental support to address the challenges with shared computing resources including computing, storage, networking and analysis, that fostered Big Data advancements.	It is extremely difficult to achieve in real-time processing.
Large data environments lack capabilities like support for massive data, high performance, high reliability, scalability, and high resource.	This paper studied features of popular NoSQL and NewSQL databases for unified storage management and quick data access.	It is extremely difficult to achieve in real-time processing.
Big data is currently the most difficult organisational problem due to the rapid generation of new data every second. Systems cannot be compatible with typical DBMS solutions.	In order to address diversity in greater detail, this article discusses current problems, possibilities, trends, and difficulties associated with big data. We'll talk about an effective fix for the huge data variety issue.	It is extremely difficult to achieve in real-time processing.

5-Cloud and mobile cloud system security issues, threats, and mitigation strategies

5.1. Concerns about Safety

One of the biggest obstacles in cloud computing settings is making sure data and programs stay secure and together. Many customers worry that their information is not completely safe on the cloud. This uncertainty stems from the absence of solid guarantees in the event of a data breach or deletion. Service Level Agreements (SLAs) that spell out legal guarantees on privacy and data protection could put these worries to rest from a legal standpoint. Since security and privacy are major concerns in the cloud, we look into innovations and best practices that can help address these challenges. Following a presentation of the most worrying assaults and dangers to cloud

computing, We are going to look into the cryptographic techniques that are currently in use that are thought to be the most effective for fending off these attacks (Gupta et al., 2015).

Many attacks targeting cloud infrastructures already exist. To that end, we detail the following assaults and threats that can significantly affect P2P cloud computing systems (Tawalbeh and Tawalbeh, 2017):

A data breach occurs when a third party obtains personal information about an individual or organization through unauthorized access to, or use of, such information in a commercial transaction. Good security practices, such as limiting hardware sharing and restricting node access to be exclusive to authorized parties, are necessary to protect P2PCS from attacks like these, which can result from user error, application vulnerabilities, or poor security settings. By taking these and other countermeasures, attackers will be unable to determine the P2PCS traffic by observing its use of individual P2PCS resources.

Encryption is a countermeasure used to prevent certain types of assaults. While encryption isn't a silver bullet for securing massive data in the cloud and mobile cloud environments, it's nevertheless widely regarded as one of the most effective methods available. If data is always encrypted, even if attackers gain access to the cloud, they won't be able to deduce any useful information.

5.2. Fundamentals of Cryptography

The most practical method of safeguarding massive amounts of data is to create systems that uphold confidentiality, integrity, and availability, the three tenets around which a security service is built. Maintaining data secrecy ensures that sensitive information cannot be accessed by any third parties. For the second option, see One aspect of data integrity is ensuring that no unauthorized changes have been made to large datasets, while another is ensuring that any calculation performed on such datasets yields accurate and consistent results. The goal of ensuring that all large data is readily available is known as "availability," and it ensures that data owners may retrieve their data whenever they need it. Applying several cryptographic techniques to the cloud infrastructure may help attain these objectives. Here, we provide a high-level summary of the approaches, directing interested parties to (Jhuria et al., 2013) and (Tawalbeh and Tawalbeh, 2017) for further in-depth discussion.

Keeping in mind the three main goals of a security service privacy, integrity, and availability during system design is the most sensible way to safeguard massive amounts of data. Data confidentiality ensures that no outside party can access, use, or see sensitive information. One aspect of data integrity is ensuring that no unauthorized changes have been made to big data, while another is ensuring that any computation performed on big data yields accurate and consistent results. The goal of ensuring big data is available is to ensure that its owners can get at it anytime they need to. Several cryptographic methods, if applied to the cloud, could help accomplish these aims. For a more in-depth discussion, please see (Jhuria et al., 2013), which we describe below.

If you keep your cloud data encrypted at all times, no unauthorized user will be able to extract any useful information from it even if they gain access to it. Symmetric-key encryption is a cryptographic primitive where the data owner must have an encryption/decryption key that can be used in either direction. Copies of this key must be disseminated before initiating encryption with symmetric-key methods, allowing for the establishment of a secure communication channel. Block encryption is the most common application for these algorithms, as they are lightning-fast

and widely employed in today's cloud and mobile cloud infrastructures. According to (Tawalbeh & Tawalbeh, 2017), the following are examples of popular symmetric encryption algorithms:
The Data Encryption Standard (DES) algorithm was cascaded to create 3DES, which is now obsolete. The average key size for 3DES is 3 * 56 = 162 bits.
Bruce Schneier created the Blowfish in 1993. Key sizes range from 32 bits to 448 bits, and it's really quick.
The Advanced Encryption Standard (AES) is the current US standard algorithm for large-scale encryption using keys of lengths 128, 192, and 256. It is the most efficient algorithm currently in use, both in terms of speed and memory usage.
Asymmetric-key encryption is another type of method used for things like digital document signing and the distribution of symmetric-key system keys. These algorithms need massive calculations on extremely sizable operands. Though they move slowly, these are highly secure, specialized algorithms. (Tawalbeh and Mohammad, 2010) provide some examples:
The RSA public-key cryptosystem was developed as a solution to the "factoring problem," the first of its kind. It was initially implemented in 1978 and has since become the standard. It is often accepted that the size of the magnitude of the modulus (the number to factorize) corresponds to the private key. For applications requiring a high level of security, keys up to 16,386 bits in length can be used, and the modulus sizes used today must be more than 2048 bits.
One of the earliest public-key protocols, Diffie-Hellman (DH) key exchange ensures the secure transfer of cryptographic keys over an insecure channel. The discrete logarithm issue in the multiplicative group of integers modulo n must be solved to use the DH technique. The minimum recommended size for a DH group for a secure key exchange is 2048 bits.
You can encrypt data, create digital signatures, and even swap keys with elliptic-curve cryptography (ECC). The elliptic curve group over finite fields and the discrete logarithm problem provide the basis for its security. In comparison to other public-key systems, ECC's key size is relatively tiny at 163 to 571 bits, as recommended by NIST for 15 of ECC's characteristics. Asymmetric encryption techniques offer a great deal of protection, but only if the modular math operations of the underlying finite fields are efficiently implemented (Tawalbeh et al., 2012; Lo'ai et al., 2004).
Hash functions, on the other hand, are algorithms for generating message digests (hash values), which are indispensable for many applications, including digital signatures. Effective software and hardware implementations of these hashing methods are available (Moh'd et al., 2010). SHA-2 and SHA-3 are two popular examples of secure hash methods.
The SHA-2 family, developed by the NSA, is a group of cryptographic hash algorithms. The previously compromised SHA-1 and MD5 algorithms served as inspiration for SHA-2. Six hash functions producing digests of 224, 256, 384, or 512 bits make up the SHA-2 family (i.e. SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256).
The Secure Hash Algorithm 3 (SHA-3) was chosen in a public competition like AES and was released on August 5, 2015. While SHA-3's digest size is configurable, predefined options include 224, 256, 384, and 512 bits.

5.3. Modern cryptography techniques

Homomorphic encryption (HE), functional encryption (FE), identity-based encryption (IBE), attribute-based encryption (ABA), verifiable computation (VC), and secure multi-party computing (MPC) are only a few examples of advanced encryption approaches that have various

advantages for handling enormous amounts of data. Instead of using public-key techniques like these, Format Preserving Encryption (FPE) is based on symmetric key encryption and is intended to retain the length or format of the original messages (keep numbers as numbers, or character sets). Secure hashing with the plaintext's original format preserved is related to Format Preserving Hashing (FPH).

When encrypting, FPE converts plaintext into ciphertext while maintaining the original format. As may be shown in (Fig.7), for instance, a social security number can be encrypted using a social security number. Feistel networks and block ciphers are the foundations of current FPE schemes. An FPE standard was published in 2016 by the National Institute of Standards and Technology (NIST) (Dworkin, 2016).

The European Union's General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) are two of the national requirements that draw organizations to FPE.

Since it is based on block ciphers, FPE is quite quick. It supports AES encryption as well as others. So while it's great for protecting sensitive information and encrypting large amounts of data, it's not so great for conducting in-depth analyses. While FPE cannot be used for aggregation (which requires homomorphic encryption) or comparisons, it may be possible to use it for other, simpler functions involving large amounts of data.

Smarter partitioning or tagging with more meta-data could enhance these features. For instance, an FPE re-encryption is not necessary for a straightforward SQL search like "select * Ek(value) (i.e. ciphertext)" or locating the most frequent value in a specific column. Finding values above or below a given threshold, however, was not as simple. Custom data partitioning (Fig.5) must be designed, not only in a simple key-value form (Fig.7) but also with more granularity and maximum separation utilizing many layers of FPE. In summing up, FPE is useful and offers adequate options for clouds with less intricate needs.

Superior public-key methods: The benefits of asymmetric approaches are numerous; for instance, with functional encryption, a user in possession of the secret key might deduce the input of the function used to encrypt the ciphertext. Some of these approaches have found niche deployments even though they generally suffer from complexity due to the extensive computations they need.

Fig.7 Fine-grained encryption (FPE) protects database fields

Homomorphic encryption (HE), verifiable computation (VC), and secure multiparty computing (MPC) are the most applicable public-key approaches for our needs. When using homomorphic encryption, computations are performed after data has been encrypted and stored in the cloud. In other words, the plaintext will never be used in any computation, just the ciphertext.

Cryp- to systems like unpadded RSA and the ElGamal cryptosystem are examples of partially homomorphic crypt-to systems (Gentry, 2009), whereas Gentry's cryptosystem and other fully homomorphic methods provide arbitrary calculations on the ciphertext produced.
When it comes to protecting sensitive information in the cloud, completely homomorphic systems are superior to partial homomorphic ones (Fig.8), and all big data analytics must be conducted on the encrypted version alone. While completely homomorphic schemes, like many modern cryptosystems, provide impressive capabilities in principle, their slow performance makes them impractical in practice. The technique is also unworkable because it needs all recipients, regardless of whether they are on the same or opposite ends, to share a single encryption key. Additionally, it only guarantees privacy on the cloud and does not permit sharing of anything beyond an encryption key, which makes it unsuitable for P2P cloud environments.

Verifiable Computation (VC) is another cutting-edge alternative cryptographic method. In VC, the prover (receiver) gets huge data or a subset of it from the data owners, processes it according to the owners' instructions, and returns the results together with proof of the accuracy of the results.

However, the advantage of verifiable computation is that the owner can check the evidence to ensure that the result is correct, even though secrecy is not provided in this system. As can be shown in (Fig.9), If the proof verification process was simpler and less expensive than performing the actual computation, it would be more efficient for the owners to handle the task themselves.
As a result, the effectiveness of this strategy is dependent on the running time of proof verification on the owner's side and the time needed to produce proof on the receiver's side. As an example of performance, the fastest time yet recorded for proof verification was 10 milliseconds (Parno et al., 2013). The time required to create a proof, on the other hand, is substantially more; for instance, 31 and 144.4 s are reported for this task in (Ben-Sasson et al., 2014) and (Parno et al., 2013), respectively. These performance metrics show that verifiable computing is still not efficient enough for big data analytics.

Secure multi-party computation (MPC) is another cutting-edge public key solution for protecting cloud-based big data. In this plan, several data owners conceal their data while simultaneously processing it in the same way. That is, all owners are concerned only with the results of the function and their data, and no owner has access to the data of any other owner.
The most efficient of the three public-key systems we discussed, multi-party secure computing (Ben-Or et al., 1988) guarantees both integrity and confidentiality. To guarantee safety when dealing with massive data over P2P clouds, it is recommended to use MPC systems due to their applicability and the ease with which they may be implemented. Confidentiality is secured during computations, but it can be easily broken if an adversary corrupts a large enough number of participants.

People seek out hardware solutions to meet their cloud system's needs because not all encryption methods are efficient. Almost all modern high-end microprocessors include hardware support for cryptographic primitives like AES and secure hash functions, although they typically lack support for public-key algorithms. While these are helpful, they typically fall short of what cloud providers want to use a tried and tested kind of encryption.

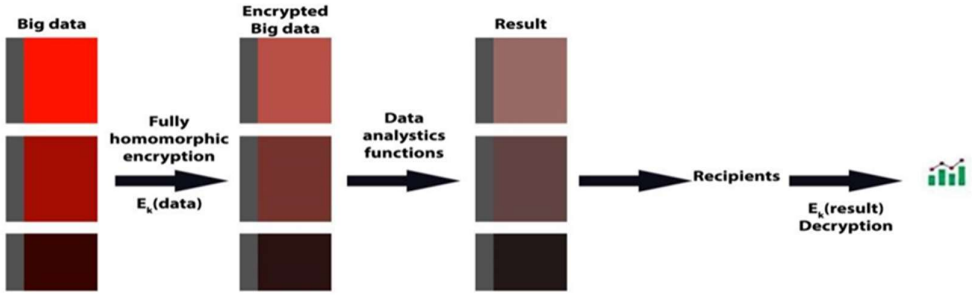

Fig.8 Homomorphic encryption is used to safeguard large dataset

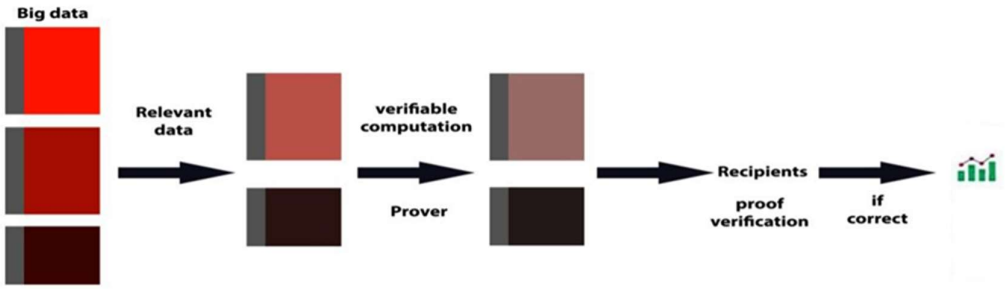

Fig.9 Safeguarding massive data with verifiable computation

10 ms were reported for proof checking in (Parno et al., 2013). The time required to construct a proof, on the other hand, is substantially longer; for instance, it was found to take 31 and 144.4 s by Ben-Sasson et al. (2014) and Parno et al. (2013), respectively. Verifiable computing still falls short of the necessary efficiency for big data analytics with these per-performance numbers.

Secure multiparty computing (MPC) is another cutting-edge public key method for protecting huge data in the cloud. This plan allows many data owners to simultaneously do the same action on their data while keeping it secret. In other words, no owner is aware of the data of others, and each owner is only concerned with the function's output and data (Fig10).

Among the three public-key systems we mentioned before, multi-party secure computing (Ben-Or et al., 1988) is seen to be the most effective because it guarantees both integrity and confidentiality. When handling huge data over P2P clouds, MPC systems are a wise choice to be used because of their practicality and ability to be applied to cloud computing systems. However, the guaranteed anonymity can be quickly compromised if an opponent manipulates enough participants in the same calculation to gain access to their confidential information.

Since not all encryption techniques are effective, users turn to hardware solutions to meet their cloud system's requirements. The majority of modern high-end microprocessors include hardware support for cryptography, such as AES and a few secure hash functions, but not any public-key algorithms. However, if cloud providers want to use a tried-and-true encryption technique, these are typically insufficient.

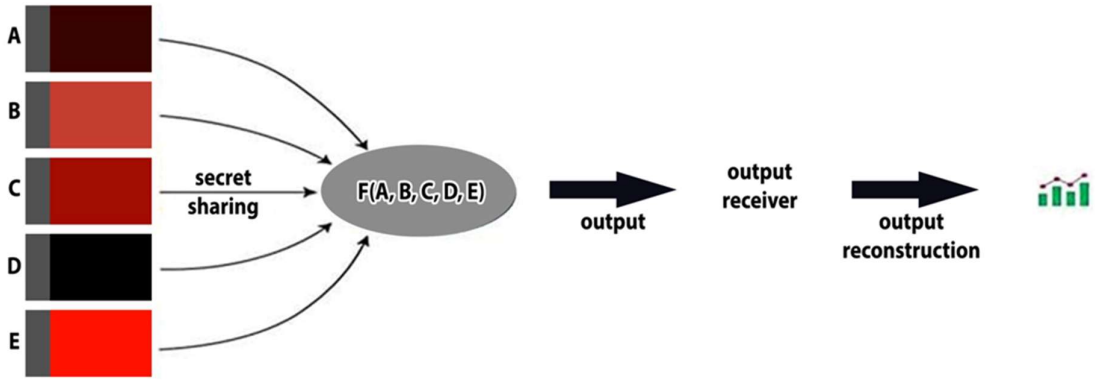

Fig.10 Securing multi-party Computing for massive data protection

5.4. An effective cryptoprocessor

One secondary and unique microprocessor known as a secure crypto-processor, secure co-processor, or crypto co-processor is responsible for delivering high throughput crypto operations to its master framework. The primary functions of a safe crypto-processor should be created after considering potential dangers and adversaries that could impair any system's functionality. Any selected security solution would have co-processor support and carry out its computations. Co-processors are crucial since they are focused solely on security issues while preserving the functionality of the systems to which they belong.

An illustration of a crypto co-processor is the Hardware Security Module (HSM) that the majority of cloud providers give as a component of their key management service (Luo et al., 2018). In tamper-resistant hardware, HSMs offer safe key storage and cryptographic operations. Therefore, these devices can identify and protect any data manipulation (most often involving encryption keys). In such circumstances, the system's internal RAM that contains any sensitive data is cleared by the secure crypto-processor.

Big data analytics may be effectively done while maintaining security thanks to Secure Crypto-Processor. They might be integrated into the cloud architecture and be in charge of all big data encryption and decryption activities. When using P2PCS, each computer node in the network can be equipped with a co-processor, like the one in (Fig.11), which will allow all encryption and decryption activities to be kept distinct from other security procedures. One issue is the cryptoprocessor-embedded hardware implementation of finite field arithmetic operations, which is entirely responsible for its efficiency (Tenca and Tawalbeh, 2004).

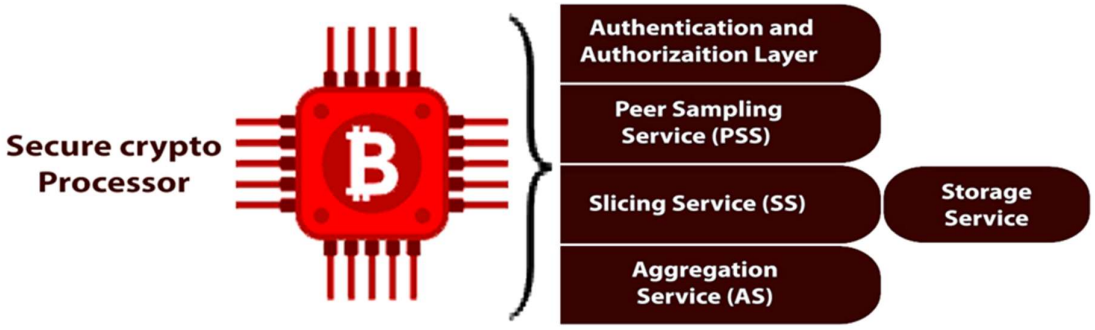

Fig.11 P2PCS architecture-supporting safe cryptoprocessor

Journal of New Zealand Studies NS35 (2023), https://doi.org/ 10.5281/zenodo.7805666

6-The suggested mobile cloud/hybrid cloud model

We provide a hybrid mobile cloud computing paradigm based on the cloudlet notion to demonstrate the theory.

Various mobile cloud computing models exist. The cooperative cloudlet model is one of these models (Bahwaireth and Tawalbeh, 2016). The enterprise cloud is utilized as a centralized, powerful infrastructure of cooperative cloudlets under the cooperative model. These cloudlets typically function at intermediate levels and collaborate to provide desired services to mobile users. The task that the user has requested should be able to be completed by the closest cloudlet (like CL1) to that user. If the service is not offered in CL1, the task request should be forwarded to the subsequent closest cloudlets, such as CL2, and so on. The user will receive the outcome via the same path that it was forwarded in return. Tasks will be forwarded to the enterprise cloud if none of the cloudlets can complete them (Bahwaireth and Tawalbeh, 2016).

The cooperative model has limitations in that, in the worst-case situation, a job must transit through every cloudlet in the model before it can be done. The task will ideally be carried out at the initial cloudlet. If the model contains N cloudlets, the task will typically cycle through N/2 of them, adding more delay and consuming more power.

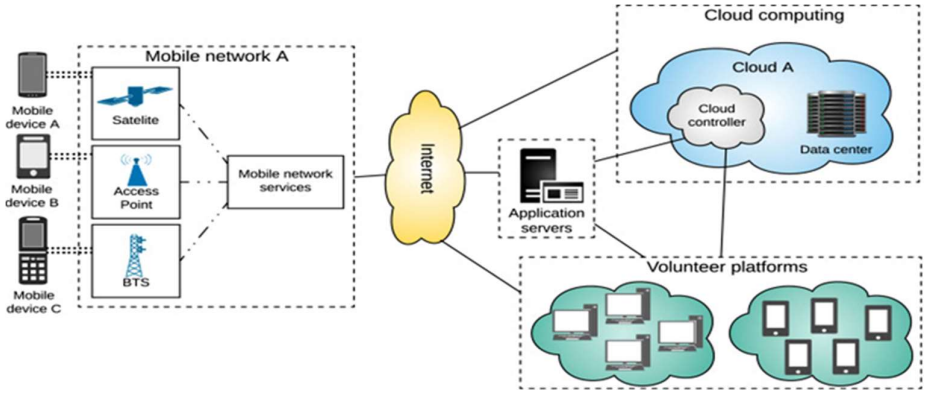

Fig.12 Model for hybrid mobile cloud computing

Another form is the centralized cloudlet model, in which a master cloudlet controls how tasks are distributed among the cloudlets by connecting them to it. This method suffers from the added delay required to distribute the task to the correct cloudlet in the model after first sending it to the master cloudlet.

We developed a hybrid cloudlet model that blends the ideas of centralized and cooperative techniques as a result of this inspiration. Additionally, we used the healthcare industry as a case study as we are learning about big data analysis using cloud computing. The proposed hybrid model is shown in (Fig.12).

We implement ideas from both the cooperative and the centralized models in the suggested hybrid paradigm. Each hospital department (clinic) has integrated the cooperative feature from our approach. One department's cloudlets collaborate to carry out the tasks that are unique to that department. In the hybrid model, a specific job will be passed through fewer cloudlets to be done than it will in the cooperative model, according to a comparison of the worst-case scenarios for the cooperative and hybrid models.

In contrast to our hybrid model, where it will only be transported within the cloudlets of that department, the job will traverse through all of these cloudlets in the hospital before it is executed.

This is because, in a single department (hybrid model), there are fewer distributed cloudlets than there are cloudlets throughout the entire hospital. Additionally, as we are leveraging the idea of a single master cloudlet, the centralized feature is applied to our model. However, we changed the duties of the master cloudlets from just routing requests to other cloudlets in the initial centralized approach to serving all common jobs coming from all hospital departments (not only particular jobs for a single clinic).

7-Simulation outputs

For cloud environments, there are various simulation tools available. The study by Bahwaireth et al. (2016) contrasts the most popular simulators and lists their benefits and drawbacks. The Mobile Cloud Computing Simulator (MCCSIM), which is primarily made for mobile cloud environments and is based on the CloudSim simulator, is used to simulate our proposed Hybrid Cloud/Mobile Cloud model. The MCCSIM interface is depicted in (Fig.13).

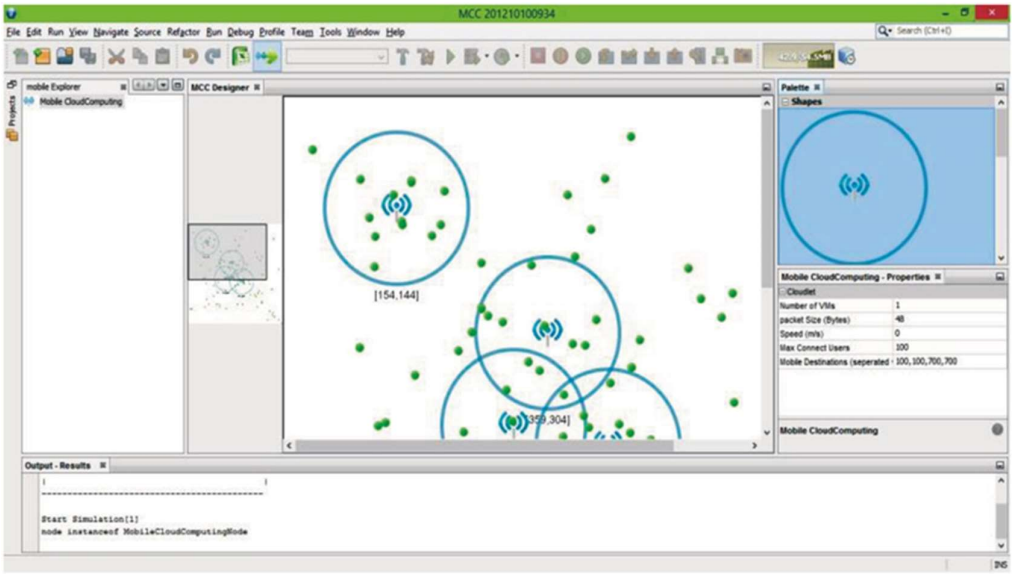

Fig.13 Interface for MCCSIM

Compared to the low load (packet size), the heavy load users consume more power and have longer delays (Fig.14). If we assume a load of 400 packets, for instance, we see that the delay is around 1.8 milliseconds. If there is only a moderate amount of traffic, say 100 packets, the delay will be less than 0.5 milliseconds. Power consumption follows the same trend, with 1 mW needed to transmit 400 packets and 0.3 mW needed for a light load of 100 packets. However, we conclude from these simulations that offloading jobs to cloudlets still results in significantly less power usage and latency than if the activities were completed locally (Lo'ai et, 2020).

Another test was done to see how much electricity mobile devices could save by adopting the cloudlet architecture. In this exercise, we use both the mobile device and the cloudlet to sort arrays. (Fig.15) demonstrates that when processing occurs locally, power consumption increases as the size of the array being sorted increases (blue curve). When the job is done in the cloudlet, it is clear that a lot of energy is saved. (Fig.15) shows that this decrease in power usage plateaus above a particular value, regardless of the size of the array being sorted.

Without a doubt, non-traditional encryption techniques will offer a high level of security for the cloud environment. However, to compare the performance of the cooperative and hybrid mobile

cloud computing models, as well as the suggested non-traditional encryption techniques discussed in the previous section, we need to characterize the task as one that will be executed in each of them (Lo'ai et, 2020).

The job is measured using the MCCSIM by the packet rate, which will be the same in both mobile cloud models and fall between 0.1 and 0.5. When implementing the same job (which symbolizes encryption), (Fig.16) displays the simulation delay and power consumption results for both the cooperative approach and our proposed hybrid model.

(Fig.16) demonstrates that, at various packet speeds, our suggested hybrid model consumes, on average, around 75% less power than the cooperative approach. Our model delays the cooperative model at specific packet rates by up to 80% less.

When the initial cloudlet that has been contacted is unable to complete the task, it is moved to the next closest cloudlet according to the cooperative model (Bahwaireth and Tawalbeh, 2016). It will be executed and sent back to the initial cloudlet if it is discovered at the following cloudlet. If not, the duty will be passed on to the third cloudlet, and so on, until it is completed. This routing method produces a longer path, increasing the delay and power usage.

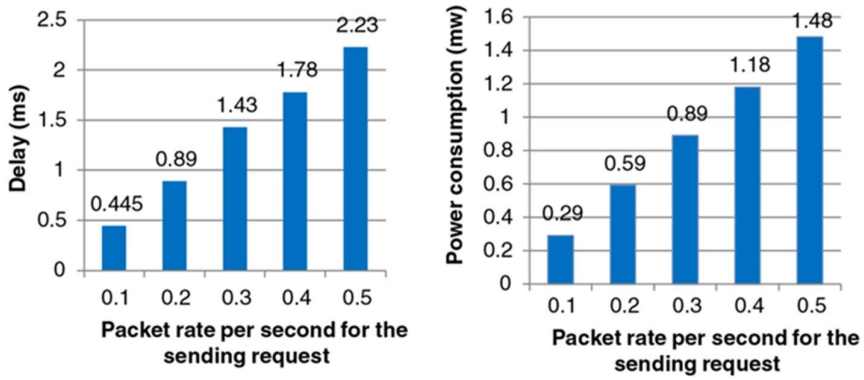

Fig.14 The effects of the cooperative cloudlet ecosystem on the mobile user's power usage and latency

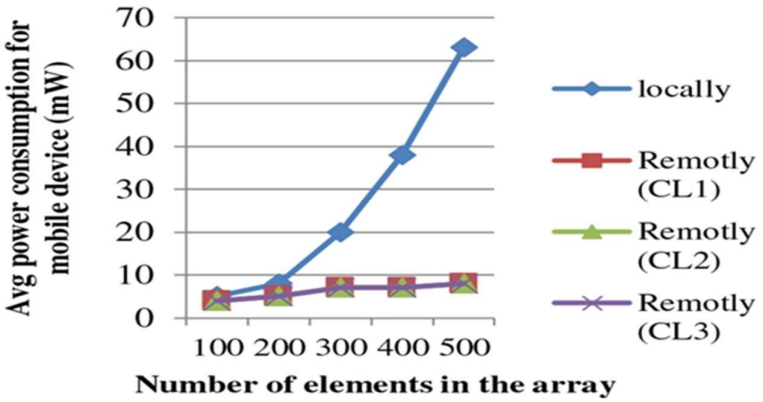

Fig.15 Power requirements for array sorting on mobile devices

Journal of New Zealand Studies NS35 (2023), https://doi.org/ 10.5281/zenodo.7805666

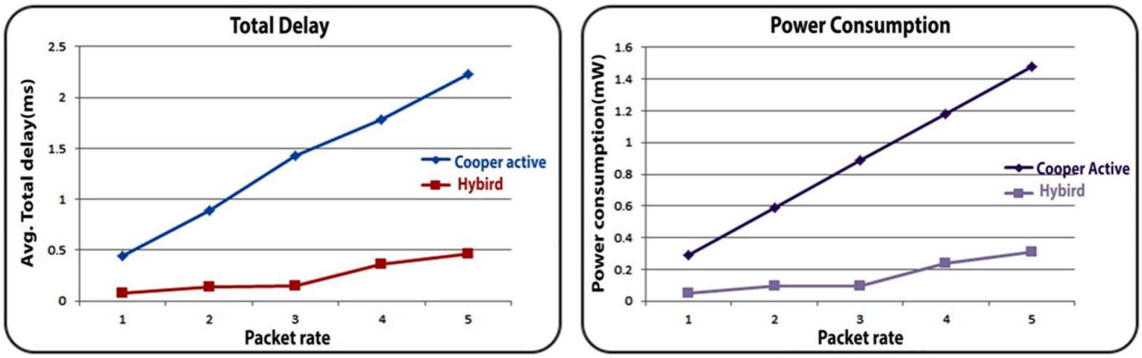

Fig.16 Cooperative and hybrid mobile cloud model comparisons

8-Conclusions and plans

Numerous computing developments offer beneficial services that improve people's lives and boost organizational effectiveness. These trends include cloud computing and mobile cloud computing, however, these technologies also come with several challenges that need to be taken into account, including user privacy and data security. In this study, we examined the most recent new technologies, such as big data and storage solutions, mobile cloud computing, P2P cloud systems, and cloud systems for the cloud. Additionally, we discussed security and privacy concerns related to these technologies and showed significant attacks that have a significant impact on cloud computing systems together with conventionally accepted solutions used to stop them.

Additionally, we looked at the layered P2PCS architecture and how crucial it is for large data analysis. Then we looked into the prospect of using fresh defenses against security threats. To secure huge data in cloud environments, we specifically presented four unique encryption techniques: format-preserving encryption, homomorphic encryption, verifiable computation, and secure multi-party computations. We also looked at the plausibility of using them in terms of performance metrics.

Additionally, to demonstrate the idea of utilizing mobile cloud computing models in actual big data applications (the healthcare instance), we suggested a hybrid mobile cloud model and ran simulations. Additionally, we assessed and compared the performance parameters (delay and power consumption) between our model and a cooperative mobile cloud model that had been previously proposed in the literature.

Finally, we draw the conclusion that large data can be hosted and analyzed in cloud and mobile cloud computing settings. Cloud and mobile cloud computing environments are under threat from a variety of established and emerging security attacks. Big data protection in these settings requires new, effective defenses. The next step would be to look at the real-time deployment of cutting-edge cryptographic techniques like Format Preserving Encryption and Homomorphic Encryption in actual cloud systems to safeguard massive data.

References

- Liu Zhong., 2023. A convolutional neural network-based online teaching method using edge-cloud computing platform in:2023 Journal of Cloud Computing:Advances, Systems, and Applications .
- Alberto Robles-Enciso, Antonio F. Skarmeta, 2023. A multi-layer guided reinforcement

learning-based tasks offloading in edge computing in: 2023 Computer Networks 220 .
- Manal Alqarni, Asma Cherif, Entisar Alkayyal , 2023.ODM-BCSA An Offloading Decision-Making Framework based on Binary Cuckoo Search Algorithm for Mobile Edge Computing in: 2023 Computer Networks 226 .
- AlDairi, A., Tawalbeh, L., 1086. Cyber security attacks on smart cities and associated mobile technologies. Proc. Comput. Sci. 109, 1086–1091.
- Ahmed Hadi Ali AL-Jumaili,Ravie Chandren Muniyandi,Ravie Chandren Muniyandi,Mohammad Kamrul Hasan ,Mandeep Jit Singh,2023. Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems: Status, Constraints, and Future Recommendations:2023. Sensors .
- Ardagna, C.A., Bellandi, V., Ceravolo, P., Damiani, E., Bezzi, M., Hebert, C., 2017. A model-driven methodology for big data analytics-as-a-service. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 10–112.
- Bahwaireth, Khadijah, Benkhelifa, Elhadj, Jararweh, Yaser, Tawalbeh, Mohammad A., 2016. Experimental comparison of simulation tools for efficient cloud and mobile cloud computing applications. EURASIP J. Inf. Security 2016 (1), 15.
- Bahwaireth, K., Tawalbeh, L., 2016. Cooperative models in cloud and mobile cloud computing. In: 23rd International Conference on Telecommunications (ICT). IEEE, pp. 1–4.
- Balasubramanian, V., Karmouch, A., 2017. Infrastructure as a service for mobile ad-hoc cloud. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–7.
- Ben-Or, M., Goldwasser, S., Wigderson, A., 1988. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, ser. STOC ’88. ACM, New York, NY, pp. 1–10.
- Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M., 2014. Succinct non-interactive zero knowledge for a von Neumann architecture. In: 23rd USENIX Security Symposium (USENIX Security 14). USENIX Association, San Diego, CA, pp. 781–796.
- Booth, G., Soknacki, A., Somayaji, A., 2013. Cloud security: attacks and current defenses Albany, NY. In: 8th Annual Symposium on Information Assurance (ASIA’13), pp. 56–62.
- Calheiros, R.N., Ranjan, R., Beloglazov, A., De Rose, C.A.F., Buyya, R., 2010. Cloudsim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and Experience 41 (1), 23–50.
- M. Dworkin, ‘‘Recommendation for block cipher modes of operation: Methods for format preserving encryption,” NIST.SP.800- 38G, Mar. 2016.
- Ferrer, A.J., Marques, J.M., Jorba, J., 2019. Towards the decentralized cloud. ACM Comput. Surv. 51 (6), 1–36.
- Gentry, C., 2009. A Fully Homomorphic Encryption Scheme (Ph.D. dissertation).
- Stanford University, Stanford, California.
- Ghasemi-Falavarjani, S., Nematbakhsh, M., Ghahfarokhi, B.S., 2015. Context-aware multi-objective resource allocation in mobile cloud. Comput. Electr. Eng. 44, 218–240.

- Gupta, D., Chakraborty, P.S., Rajput, P., 2015. Cloud security using encryption techniques. Int. J. Adv. Res. Comput. Sci. Softw. 5, 425–429.
- Jelasity, M., Voulgaris, S., Guerraoui, R., Kermarrec, A.-M., van Steen, M., 2007.
- Gossip-based peer sampling. ACM Trans. Comput. Syst. 25 (3).
- Jelasity, M., Montresor, A., Babaoglu, O., 2009. T-man: gossip- based fast overlay topology construction. Comput. Netw. 53 (13), 2321–2339.
- Jemal, H., Kechaou, Z., Ayed, M.B., Alimi, A.M., 2015. Mobile cloud computing in healthcare system. In: Núñez, M., Nguyen, N.T., Camacho, D., Trawinski, B. (Eds.), Computational Collective Intelligence. Springer International Publishing, Cham, pp. 408–417.
- Jhuria, M., Singh, S., Nigoti, R., 2013. A survey of crypto- graphic algorithms for cloud computing. Int. J. Emerg. Technol. Comput. Appl. Sci. 05, 141–146.
- Kahanwal, B., Singh, T.P., 2013. The distributed computing paradigms: P2P, grid, cluster, cloud, and jungle. CoRR.
- Kumari, Priti, Kaur, Parmeet, 2018. A survey of fault tolerance in cloud computing. J. King Saud Univ.-Comput. Inf. Sci.
- Kurdi, Heba A., 2015. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems. J. King Saud Univ.-Comput. Inf. Sci. 27 (3), 315– 322.
- Liroz-Gistau, M., Akbarinia, R., Pacitti, E., Porto, F., Valduriez, P., 2013. Dynamic workload-based partitioning algorithms for continuously growing databases. Trans. Large-Scale Data- Knowledge-Centered Syst. 12, 105–128.
- Liu, J., Ahmed, E., Shiraz, M., Gani, A., Buyya, R., Qureshi, A., 2015. Application partitioning algorithms in mobile cloud computing: taxonomy, review and future directions. J. Netw. Comput. Appl. 48, 99–117.
- Lo'ai Tawalbeh, Mohammad A. Tawalbeh, Monther Aldwairi,2020 . Improving the impact of power efficiency inmobile cloud :2020 . John Wiley & Sons, Ltd.
- applications using cloudletmodel
- Lo'ai, A.T., Bakhader, W., Mehmood, R., Song, H., 2016. Cloudlet-based mobile cloud computing for healthcare applications. In: 2016 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1–6.
- Lo'ai, A Tawalbeh, Tenca, Alexandre F., 2004. An algorithm and hardware architecture for integrated modular division and multiplication in GF (p) and GF (2n). In: Proceedings of the Application-Specific Systems, Architectures and Processors, 15th IEEE International Conference, pp. 247–257.
- Lo'ai, A Tawalbeh, Bakhader, Waseem, 2016. A mobile cloud system for different useful applications. In: Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, pp. 295–298.
- Luo, S., Hua, Z., Xia, Y., 2018. TZ-KMS: a secure key management service for joint cloud computing with ARM TrustZone. In: IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 180–185.
- Mohd, Abidalrahman, Aslam, Nauman, Marzi, Hosein, Tawalbeh, L.A., 2010. Hardware implementations of secure hashing functions on FPGAs for WSNs. Proceedings of the 3rd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT).

- Mollah, M.B., Azad, M.A.K., Vasilakos, A., 2017. Security and privacy challenges in mobile cloud computing: survey and way ahead. J. Netw. Comput. Appl. 84, 38– 54.
- Oussous, Ahmed, Benjelloun, Fatima-Zahra, Lahcen, Ayoub Ait, Belfkih, Samir, 2018. Big data technologies: a survey. J. King Saud Univ.-Comput. Inf. Sci. 30 (4), 431– 448.
- Parno, B., Howell, J., Gentry, C., Raykova, M., 2013. Pinocchio: Nearly practical verifiable computation. In: Proceedings of the 2013 IEEE Symposium on Security and Privacy, ser. SP '13. IEEE Computer Society, Washington, DC, USA, pp. 238–252.
- Tawalbeh, Lo'ai, Jararweh, Yaser, Mohammad, Abidalrahman, 2012. An integrated radix-4 modular divider/multiplier hardware architecture for cryptographic applications. Int. Arab J. Inf. Technol. 9 (3).
- Tawalbeh, L.A., Mohammad, Abidalrahman, Gutub, Adnan Abdul-Aziz, 2010. Efficient FPGA implementation of a programmable architecture for GF (p) elliptic curve crypto computations. J. Signal Process. Syst. 59 (3), 233–244.
- Tawalbeh, L.A., Tawalbeh, H., 2017. Lightweight crypto and security. In: Song, H., Fink, G.A., Jeschke, S. (Eds.), Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications. Wiley, pp. 243–261.
- Tenca, Alexandre F., Tawalbeh, L.A., 2004. Algorithm for unified modular division in GF (p) and GF (2n) suitable for cryptographic hardware. Electron. Lett. 40 (5), 304–306.
- Wang, J., Zhang, W., Shi, Y., Duan, S., Liu, S., Industrial big data analytics: Challenges, methodologies, and applications, https://arxiv.org/pdf/1807.01016.pdf, April 2018.
- Yaqoob, I., Ahmed, E., Gani, A., Mokhtar, S., Imran, M., Guizani, S., 2016. Mobile ad hoc cloud: a survey. Wireless Commun. Mobile Comput. 16 (16), 2572–2589.
- Liu, Y.; Liang, S.; He, C.; Zhou, Z.; Fang, W.; Li, Y.; Wang, Y. A Cloud-computing and big data based wide area monitoring of power grids strategy. IOP Conf. Ser. Mater. Sci. Eng. 2019, 677, 042055.
- Javed, A.; Larijani, H.; Ahmadinia, A.; Gibson, D. Smart Random Neural Network Controller for HVAC Using Cloud Computing Technology. IEEE Trans. Ind. Inform. 2017, 13, 351–360.
- Rao, S.N.V.B.; Yellapragada, V.P.K.; Padma, K.; Pradeep, D.J.; Reddy, C.P.; Amir, M.; Refaat, S.S. Day-Ahead Load Demand Forecasting in Urban Community Cluster Microgrids Using Machine Learning Methods. Energies 2022, 15, 6124.
- Wang, H.; Sun, J. Quantitative analysis of data mining application and sports industry financing mechanism based on cloud computing. Int. J. Grid Distrib. Comput. 2016, 9, 233–244.
- Yuan, J. An Anomaly Data Mining Method for Mass Sensor Networks Using Improved PSO Algorithm Based on Spark Parallel Framework. J. Grid Comput. 2020, 18, 251–261.
- Jia, X. Research on network abnormal data flow mining based on improved cluster analysis. Distrib. Parallel. Databases 2021, 40,797–813.
- Eddoujaji, M.; Samadi, H.; Bohorma, M. Data Processing on Distributed Systems Storage Challenges. In Smart Innovation, Systems and Technologies; Springer: Berlin, Germany, 2022; Volume 237, pp. 795–811.
- Naeem, M.; Jamal, T.; Diaz-Martinez, J.; Butt, S.A.; Montesano, N.; Tariq, M.I.; De-la-Hoz-Franco, E.; De-La-Hoz-Valdiris, E. Trends and future perspective challenges in big data. In Proceedings of the Advances in Intelligent Data Analysis and Applications, Arad,

Romania, 15–18 October 2019; pp. 309–325.
- Amir, M.; Haque, A.; Kurukuru, V.S.B.; Bakhsh, F.; Ahmad, A. Agent based online learning approach for power flow control of electric vehicle fast charging station integrated with smart microgrid. IET Renew. Power Gener. 2022.
- Shariff, S.M.; Alam, M.S.; Faraz, S.; Khan, M.A.; Abbas, A.; Amir, M. Economic approach to design of a level 2 residential electric vehicle supply equipment. In Advances in Power and Control Engineering: Proceedings of GUCON; Springer: Singapore, 2020; pp. 25–40.