Article

A Case Study of Docker Based Databases and Why they Should Become an Alternative to Centralised Databases

Ade Ajasa * , Hassan Chizari , Abu Alam

Posted Date: 16 July 2025

doi: 10.20944/preprints202507.1379.v1

Keywords: databases; security; performance

Article

A Case Study of Docker Based Databases and Why They Should Become an Alternative to Centralised Databases [†]

Ade Dotun Ajasa *, Hassan Chizari and Abu Alam

[1] University of Gloucestershire, School of Computing & Engineering, The Park, Cheltenham, GL50 2RH, United Kingdom.

[*] Correspondence: adeajasa@connect.glos.ac.uk

[†] This work is the PhD research of Ade Dotun Ajasa supervised by Hassan Chizari and Abu Alam.

Abstract

Data leakage, cyber threats, insiders who misused their account privileges and external and also internal threats to a database just, to mention a few of the problems affecting a centralised database in today's world of cloud computing and the Internet. We proposed to install two different types of databases which, are hosted on the Internet into the Docker engine then from the data collected we, would present a graphically output of the findings. We discovered from the findings that, the Docker engine had its short comings but, could be improved when used with an expensive and powerful computer.

Keywords: databases; security; performance

1. Introduction

Problems with a centralised database:-

- External and also internal threats to a database.
- Users abuse their privileges which could have been gained legally or obtained illegally.
- Audit logs can not always be depended on.
- Discovering breaches are extremely difficult.
- Insiders who misused their account privileges.
- Lost or stolen devices that hold the data of employees.
- Data leakage and cyber threats.
- The Internet.
- Data breaches and database security.
- Data privacy.
- Cyber security measures which are insufficient.

Authors of the research paper Zhao et al. [1] highlighted the problems associated with data breaches in a database in 2016. Real time processing is accomplished when using a database that is designed for real time processing, this means it can deal with constantly changing workloads. On top of that, there has been more external and also internal threats to a database. To simplify, commercial secrets, bank details and personal privacy are some of the things stored in these databases Zhao et al. [1].

Referring to the views of the research paper Wagner et al.[2], published in 2017 also supported the authors of the research paper Zhao et al. [1] which, was published in 2016. However, a Database Management Systems (DBMS) is used to process and store users data. Security mechanisms and access controls such as audit logs can not always be depended on. Moreover, users have been know to abuse their privileges which could have been gained legally or obtained illegally.

A database needs to be able to detect any breach within the database urgently and collect evidence relating to such attack Wagner et al.[2]. According to the authors of the research Said et al. [3], in 2020 insiders who misused their account privileges is one of the most constant cause of data breaches in a database and discovering such breaches are extremely difficult. The authors of this research paper Said et al. [3] proposed the Negative Selection Algorithm from artificial immune system mechanisms and the Danger Theory model which are based on an adaptable efficient database intrusion detection algorithm Said et al. [3]. Furthermore, Negative Selection Algorithm and Danger Theory figure are types of Intrusion Detection Systems (IDS), these devices are deployed to protect computer networks. According to the research paper Tahir et al. [4], Intrusion Detection Systems (IDS) is a very important network deference used with computer networks Tahir et al. [4].

In view of, the authors of these two research papers Neto et al. [5] and Algarni et al. [6] published in 2021 still highlighted the same problems associated with data breaches and database security. Another key thing to remember, data leakage and cyber threats had increased because of increase in data usage regarding the Internet. Also, the authors of the research Neto et al. [5] looks at the data breaches of personal information in database between 2018 to 2019 Neto et al. [5], Said et al. [3]. To demonstrate, in 2019 the exposure of confidential and critical information of the customers of Capitol One due to a cyber attack on their database Neto et al. [5] likewise, the authors of the research Algarni et al. [6] also published in 2021 elaborated on modern business systems breaches and cyber security risks. Initially, a cyber security solution would limit the attacks against a database storage. Also, security leaks could be the result of lost or stolen devices that hold the data of employees, which could be security credentials leaked by human error. To clarify, some of the cyber attacks could be cross-site scripting (XSS), privilege escalation and Structured Query Language injection attacks (SQLi). The input of well crafted malicious code in Structured Query Language (SQL) statements via the input of a web page could destroy a database Algarni et al. [6].

On the contrary, the authors of theses two research Wang et al. [7] and Hassanzadeh et al. [8] also published in 2021 gave a stark review on the data breaches and database security as compared to, the authors of these two research papers Neto et al. [5] and Algarni et al. [6] . However, database breaches have become a security problem that is widespread, 3950 database breaches were globally reported in November 2018 and October 2019 while, 60% of victims identity were leaked due to 1665 breaches on different credential databases Wang et al. [7]. The current debate about, how data breaches and personally identifiable information gets into the hands of unauthorised personnels which, has caused serious concerns among companies and individuals since it has now become a common problem. To this end, database breaches such as Yahoo in 2013 and 2014, LinkedIn in 2012, Marriott International in 2014 and 2018, Equifax in 2017 and many more show that there are institutions or companies that still have a habit of practising cyber security measures which are insufficient, despite the improvement and awareness of security mechanisms Hassanzadeh et al. [8].

Similarly, in 2021 Non Structured Query Language (NoSQL) databases have not escaped the clutches of hackers. NoSQL databases store their data in a different format than relational tables. Moreover, first introduced the databases disrupted the database market. On top of that, NoSQL databases could handle features like scalability, performance and availability, unfortunately compromises had to be made to attain these goals. NoSQL databases handle unstructured data, data that is not organised in a pre-defined manner or pre-defined data model that said, privacy related features were compromised. Data privacy means having the right on how data is disclosed or collected. Therefore, you can not ignore data privacy that easily Goel et al. [9].

The following structure represents how this research paper is laid out: Section 1 explains the security problems affecting a centralised database. Section 2 a look at why we need to remember what had happened in the past when, peoples rights and data where used against them. Section 3 an explanation of the security breaches in centralised databases. Section 4 a link between cloud computing and security, security vulnerabilities, security misconfiguration of the database and the consequences of having unpatched Software on the database system is explored in this section. Section 5 We are introduce to the Docker engine, the architecture of the Docker engine, a look at Linux mobile phones that come with Docker installed in them and Docker updates and unpatched software are explored in

doi:10.20944/preprints202507.1379.v1

this section. Section 6 in this section we, examine the what happens when profit is put before security in a database system. Section 7 how the data was collected is presented in this chapter. Section 8 a look at the performance from the data collected and the trade off's involved. Section 9 elaborates on the summary of findings. here we justify based on the evidence gathered from the collected data that, a Docker database is far more better than the centralised database. Section 10 This brings a conclusion to this research paper.

2. What Is the Motivation Behind This Research

To begin with, the motivation to take on this research topic was, the ability to use open source software to tackle a real life menace in regards to performance and security of users data hosted in a centralised database and also, the centralised database itself. Above all, this affects everybody, irrespective of where they reside or who they are, be they rich or poor. Most importantly, users should have the right to own their data by default, if the history of the past years has taught us anything Miyamoto [10], Seidelman [11].

3. The Centralised Database and Security

Firstly, a collection of data that is organised is what a database can be known as. The information that is held on a database could be described as an important and valuable corporate resource. Secondly, a database allows the administrator to modify, create, query and delete user data. When data is transmitted across sites, protection to the user data could come in the form of electronic signatures or encryption. Lastly, the collective measures used to secure and protect a database refers to it's security Zaw et al. [12] however, there needs to be an elevation of the possibility of the use case where users will need to frequently have access to data, in order to closely give real world scenarios Santos et al. [13].

Considering, in the world of today data is money, the world is driven by data across many different geo-distributed (Spread across multiple geographical regions) clouds and has to be collected efficiently. Additionally, when under high loads, data should be accessed on a consistent basis even during the presence of failures. Almost every small owned business, companies and institutions, depend on larger data analytics to optimise their business logic. Furthermore, the traditional database services has now moved online. In other words, a database is an organised collection of user data. After all, if the security employed to the database is capable of protecting the data that it is hosting, malicious attacks or threats from hackers can be stopped from stealing the data, this was said in 2021 by the authors of the research paper Crooks et al. [14] although, in 2016 an investigation on how to build a database that would not be vulnerable to internal or external attacks was proposed by the authors of the research paper Toapanta et al. [15].

Meanwhile, it is possible to consider network problems and extremely high computer loads with the introduction of modern applications however, there has to be a continuity in the flow of data which leads to service been guaranteed. The constant evolving Information Technology (IT) services scalability and availability is why Docker containers can be of a high value to the Information Technology (IT) industry Perri et al. [16]. Moreover, the authors of the research paper Perri et al. [16] decided to include Service Level Agreement (SLA) within its implementation. Service Level Agreement (SLA) simply put, is the type of services that a service provider would provide and the type of services provided, this is basically a contract service-level agreement (SLA). Hence, this robs the users of the autonomy or the right of governing their self. The authors of the research paper Said et al. [3] gave examples of database and data breaches from 2016 - 2020 Said et al. [3]. Additionally, an up to date information can be accessed on database and data breaches at these websites Data Breaches That Have Happened in 2022, 2023 and 2024 So Far. and Recent Data Breaches - 2023. Also, the authors of the research paper Nelson et al. [17] goes into details of the problems with a centralised database and has provided an up to date web page on the current breaches within databases around the world Cyber Security Data Breaches Nelson et al. [17].

In view of, the consequence of the security of a traditional database will always be disastrous when it's security is compromised. Moreover, a look at a decentralised database is in need to see how it stands-up to an attack from criminals, hackers and intruders who are external from the traditional database. Web services and Internet of Things (IoT) are associated with Information and Communications Technologies (ICT) while, user data also plays an important role. User data is very difficult to protect when held on a centralised database because, the centralised database has always been a centre point of failure. Where a centralised database is concerned, integrity, confidentiality and availability can be seen as important threats. Severe damage to the database data integrity can occur when illicit authentication and authorisation has taken place because, the violation of data confidentiality by hackers has successfully been tampered with. Furthermore, hackers or criminals only have one objective in mind and that is to compromise the centralised database but, this would be impossible to achieve in a decentralised network Ding et al. [18] despite this, we still need to investigate how to build a security framework around a database that would not be vulnerable to internal or external attacks Toapanta et al. [15].

In other words, the handling of the privacy of users information and the security that is needed to keep the users information safe should be, held by a database institution. Because of the security risks that are associated with a cloud based infrastructure, mission critical data that belongs to institutions would rather be kept on site instead of in the cloud Samaraweera et al. [19]. Likewise, an attacker or hacker would tend to alter the log files of a database especially, the transactional history log file, if the so called attacker or hacker gains access to a database via unauthorised access. To bring about a limit to the functionality of the server by, removing access for users to run certain commands and this, would be a way to provide a higher level of security Nash et al. [20].

4. Cloud Computing and Database Security

Firstly, data security is an integral and important part of cloud computing. Secondly, Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) are different models with various architectures in reference to cloud computing. Thirdly, it's capacity, accessibility and flexibility are some of the advantages of cloud computing when, compared with the traditional way of keeping data and online computing. Fourthly, just like in any area within computing, cloud is not without it's fair share of security issues, issues experienced by clients and service providers. Moreover, sharing of uploads is a common risk to cloud computing and the security of the clients data is the responsibility of the cloud providers Lee et al. [21].

Considering, web applications are data driven in today's world. Users are able to manoeuvre and manipulate their data, due to the increase in companies and institutions moving their data online. The more web applications that have being developed, has unfortunately brought with it the rise in database security Odirichukwu et al. [22]. Furthermore, lack of incentives for good security, there is hardly or no training of developers in security testing, monitoring database transactions and log files are inadequate while, there are none review practices and non access policies. To put it more simply, there are no government policies regarding data and usage theft because, of accessibility and high cost that results in the use of low end Internet security, the rotation of user account credentials does not exist and short deadlines create loopholes in the security of web applications these, reasons are because developers are spending so little time to enforce security in web applications Odirichukwu et al.[22].

Moreover, web applications are used for everyday activities on the Internet by people which, has lead to the hackers focusing their attention on these web applications to get access to any database via the Internet. In particular, a web application that has not been properly implemented could lead to it been exploited by these hackers which, could lead to confidential data stolen Deepa et al. [23]. Initially, a vulnerability was registered as CVE-2019-15126 details in the National Vulnerability Database NVD. Secondly, this security vulnerability has asked questions about how secure is Internet of Things (IoT) devices like mobile phones, laptops, databases and smart watches when they are attached to a wireless network. Internet of Things (IoT) has helped people to take the advantage of using different types of devices that connect to the Internet within a wireless network.

Finally, the convenience and ease that these people have gained could also be exploited by hackers or criminals because these devices are prone to problems associated with security According to National Vulnerability Database NVD CVE-2019-15126, caused billions of Wi-Fi devices to get affected. Most devices are a risk in terms of security and a vulnerability on the Internet when used with Internet of Things (IoT). Cyber attacks have increased while, many types of vulnerabilities are discovered every day, this has been accelerated by the vulnerabilities relating to the software been used. On top of that, in a database the software used is of no exception. Proof that there is justification that theses vulnerabilities do exist, can be found at The Common Vulnerabilities and Exposures CVE website. Referring to the reviews of the authors of the research paper Park et al. [24], nearly all mobile phones provide an Application Programming Interface (API) for apps and also store their data on a database, the Application Programming Interface (API) is used to gain access to the database. Most of the things done on a mobile phone are via the Application Programming Interface today's world, they retain our business and personal information and could be classified as a movable storage Park et al. [24].

4.1. Abuse of Authority With Security Misconfiguration of The Database and Unpatched Security Vulnerabilities

An alternate argument, with regards to the author of the research paper Gao et al. [25], in relation to having a cost effective database, backing up and collecting users data should start from each individual who owns their user data and at the same time each individual user has constant access to their data and evaluate the secure framework with the use case where users will need to frequently have access to data in order to closely give real world scenarios Santos et al. [13]. In contemplation of, institutes and organisations like that of the education sector, the health sector and the business sector, have in the last three decades relied on the use of a database to store their data securely Khan et al. [26]. Irdeto secures applications and platforms for connected health, Internet of Things (IoT) connected industries, video games, video entertainment and connected transport Irdeto. Moreover, discovered in April 2018, Irdeto reported that 15 places on the dark web, consisting of 69 different sellers, were selling 854 users personal credentials of people who had subscribed to 42 different services like, Hulu, Netflix, DirecTV, HBO and PlayStation were exposed to a similar hack on their network while, users data like phone numbers, credit card details, date of birth details, contact addresses and other important data were stolen Elem et al. [27].

Referring to the views of the authors of the research paper Uijie et al. [28], a database is the foundation and core when it comes to an information system while, security auditing is an important part of the database. What makes a database attractive to hackers and criminals is the users data that is kept in the database. To clarify, one of the opportunities that hackers and criminals have exploited too such a large degree is the fact that, most databases have too many interfaces. There must be a safe security framework to stop or minimise attacks by internal staff who have legitimate access to work within the premises mostly, the administrators who are legally authorised to access the database Uijie et al.[28], having said that, this is why this thesis will investigate how to build a security framework around a database that would not be vulnerable to internal or external attacks Toapanta et al. [15].

Meanwhile, the high cost in data management is because of the cost associated to each institutions, industries and when it comes to exchange of information between these institutions or industries, this aspect is lacking. These institutions or industries still use the traditional management method in their collection of data. To give an illustration, archive rooms or even reference rooms would eventually become their database. The problems that occur when you have this type of database are, data collected and its accuracy, data update and looking for the data. For instance, with the advantages that can be derived from Internet big data, the construction of a management database would be cost effective. We can eliminate the limitations of space and time with a management database that can collect all the data of an institution or industry Gao et al. [25].

Considering, the cause of most data breaches within a database is the insiders who misuse the account privileges assigned to their account. It is very difficult to find out these types of breaches. Confidential users data are extremely vital to both the individual user and also users belonging to different institutions. Finally, the definition of a data breach is a user gaining unauthorised access to data that the user has no right to and could be intentionally or by an accident Said et al. [3]. To put it another way, confidentiality data breach, availability data breach and integrity data breach are types of data breach. Moreover, the result that would lead to a bad reputation with significantly financial loss for that institution could be the result of the importance of a data breach at cooperate level. To clarify, authorisation abuse, weak authentication, information misuse and insider privileges of account misuse are the important reasons there has been so many high level data breaches. Another key thing to remember, the results of the misuse of a privilege account that has legitimate authority to access areas in a database could be, the misuse of a privilege account, legitimate privilege abuse, inappropriate privilege abuse and unauthorised privilege promotion Said et al. [3].

4.2. The Consequences of Unpatched Software

One aspect which illustrates, in 2022 the problems associated with data breaches and database security continued to get worse according to the authors of these research papers Jusak et al. [29], Kalkman et al. [30] and He et al. [31]. Although, the move to public cloud servers within the medical institutions, the public cloud servers were prone to breach of privacy and security. Moreover, users were more concerned about privacy and security because, malicious users could have access to data that does not belong to them. Additionally, internal threats needed to be looked into very closely especially when the users involved have administrative rights to the database while, such type of users are key managers, programmers and engineers Jusak et al. [29]. Yet, the abuse of patients data, breaches of confidentiality and data security transparency are views the public and especially patients might have, regarding sharing of their data within the health sector Kalkman et al. [30].

On the other hand, the authors of the research paper Kalkman et al. [30] is supported by the authors of the research paper He et al. [31]. Furthermore, over the past five years, more than one hundred and fifty four million health records in total have been hacked which resulted to thousands of data breaches, in relation to health care that was reported. As evidence, in the United Kingdom (UK) a ransomware attack called WannaCry malware, caused nineteen thousand appointments to be cancelled with the National Health Service (NHS) which resulted in the loss of £20.000.000 between 12.06.2020 and 19.06.2020 but, upgrades to the National Health Service (NHS) IT systems and the clean-up that followed cost £72.000.000 He et al. [31].

On top of that, the authors of the research paper Hassanzadeh et al. [8] published in 2021 mentioned Equifax as one of the companies that had it's users data breached in 2017 and furthermore, according to a research paper Neto et al. [5] which, was also published in 2021 mentioned that Capitol One was a victim of a cyber attack on their database in 2019 yet, the authors of the research paper Khan et al. [32] published in 2023 refers to the 2019 data breach in Capital One as a data breach that affected over 100 million individuals who had the security and privacy of their personal information breached, the worst data breach since the data breach that occurred in the companies Marriott, Target and Equifax. Hence, in the past decade the number of data hacks has increased Khan et al. [32].

Another key thing to remember, the authors of these research paper Liu et al. [33] and Li et al. [34] both published in 2023 said, receiving world wide attention is hackers stealing confidential data. In addition, Stephen P. Teale Data Center in California had a massive data breach on 05.04.2002 by a hacker which, resulted in two hundred and sixty five thousand state employees personal identities been compromised Liu et al. [33] while, an eye clinic in Singapore on 06.08.2021, had the medical records that belonged to seventy three thousand patients involved in a data breach due to ransomware attacks in contrast, to Dedalus Biologie who were fined €1.5 million on 23.02.2021 by the (European Data Protection Board, 2022), for having a massive breach in their medical data which affected half a million people Li et al. [34].

doi:10.20944/preprints202507.1379.v1

5. The Introduction of Docker

According to the authors of the research paper Vinicius et al. [35], the architecture of Docker enables it to build environments that are virtualised in a way that is isolated. However, the cost associated with the resources of the host computer are reduced because, Docker shares the same kernel as the host computer and this also, increases performance. Additionally, Docker images can be downloaded from Docker repositories Vinicius et al. [35]. Launching a Docker image after the image has been downloaded from repository, creates a container which can be deployed at anytime, since it resides in the computers local cache. Furthermore, the owner of the container can delete the container when they want too Ahmed et al. [36].

5.1. Docker Architecture

Primarily, Docker has four main internal components:-

- **Docker Images** - Firstly, an image can be built in two methods. Using a read-only template is the first method this, is always a base template of the operating system it is built on. To give an illustration, Ubuntu 20.04 when built would only contain the base elements to operate as an operating system. Additionally, creating a Docker file is the second method. This method requires instructions or commands written in a file and when, this file is run in a Linux terminal, this will then build an image Rad et al. [37].
- **Docker Containers** - Secondly, Docker containers are created from a Docker image. These containers are run in isolation in other words, the Docker containers are mirror images of the Docker image Rad et al. [37].
- **Docker Registries** - Thirdly, Docker images are placed in docker registries. These images can be either pushed or pulled from a single source. On top of that, there are private and public registries. Docker hub is known as a public registry where, images can be freely uploaded or downloaded Rad et al. [37].
- **Docker Client And Server** - Lastly, Docker is a client and server based application Rad et al [37].

To clarify, unlike the function of Docker explained by the authors of the research paper Rad et al [37] importantly, the authors of the research paper Pratap et al. [38] expands on the function of Docker. Operating system level virtualisation and hardware system level virtualisation are the two types of virtualisation technology used in a Data Center environment. In the operating system level virtualisation containers are created by resources been virtualised within the operating system which, is made up of operating systems libraries and their dependencies. Docker containers are a type of operating system virtualisation. But, in a hardware system level virtualisation the server's resources are virtualised into multiple virtual machines by a hypervisor. On top of that, to run different types of applications, each virtual machine has its own libraries and operating system. KVM (Kernel based virtual machine and a full virtualisation solution for Linux) and Xen (A type-1 hypervisor) are examples of a hardware level virtualisation. Figure 1 Pratap et al. [38].

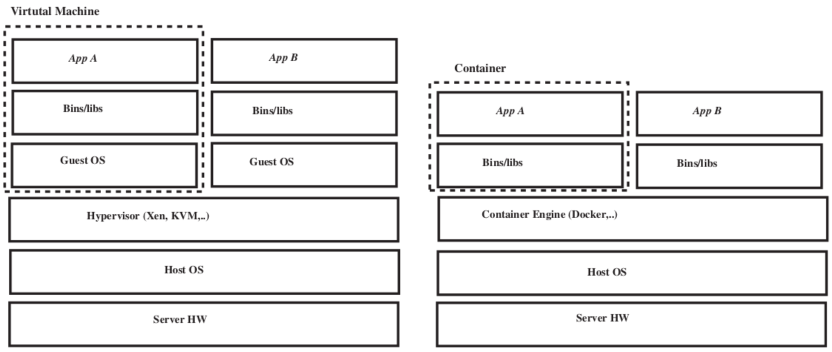

Figure 1. Virtual Machine Vs Container Pratap et al.[38]

Additionally, containers host the applications that are deployed to them automatically while, Docker can be refereed to as a light weight container-based technology. Containers are software packages and allow the building, shipping and distribution of applications developed by developers. Figure 2 is made up of a Docker Client, Docker Daemon and Docker Registry. The user inputs commands from the Docker client which acts a primary interface. The Docker Registry represents a server. A connection is established between the Docker client and Docker Daemon while, the Docker Client controls the host machine makes, a request when it wants to create an image then, publish any images that have been requested while managing the running containers that have been executed. The containers are instances created from the Docker images. Containers are deployed by the Docker Daemon which looks after the monitoring, stopping, pausing, running and killing of any container. The Docker Daemon responsibility is also building and storing of the images. The Docker Registry handles both the customised private, public and pre-built images. The Docker Registry also distributes and stores images Pratap et al.[38] as evidence, the authors of the research paper Musleh et al. [39] shared their Docker, Datasets and Application Programming Interface (API) on the Docker Registry Musleh et al. [39].

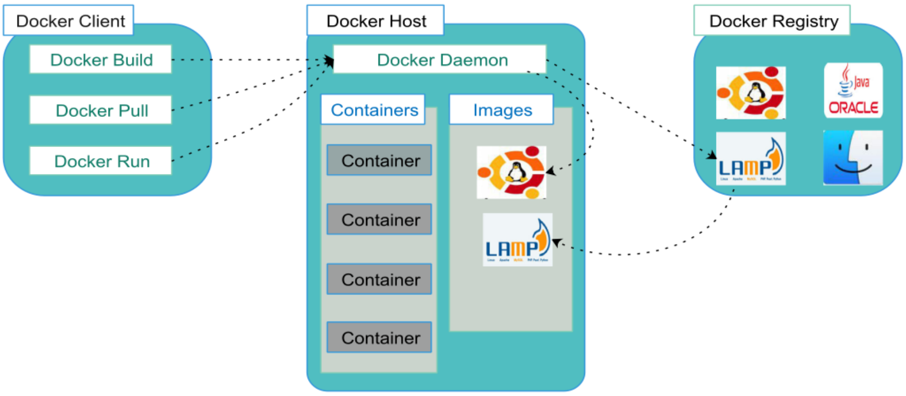

Figure 2. The Architecture Of Docker Pratap et al.[38]

5.2. Linux Mobile Phones That Ship with Docker Installed

Primarily, there are three popular mobile phones that ship with Linux pre-installed as their main operating system Pine64. Pine64 is shipped with the Linux operating system called Manjaro yet, a different distribution (operating system) can be installed by the owner of a Pine64 or PinePhone Pro. PinePhone Pro is bundled with the Linux operating system called Sailfish OS (Operating System) but, just as the Pine64, a different distribution (operating system) can be installed by the owner of a PinePhone Pro. Librem 5 comes installed with PureOS operating system Librem 5 Want et al. [40]. According to the authors of the research paper Qian et al. [41], the popularity of mobile phones has brought with it an ugly side which is, the increase of security threats to mobile phone applications. Database has always been an area of security that needs a looking into. Hacking to find out a users location, the hijacking of a users transactions and communications, a users contacts, exploiting the mobile devices cache and exploiting of mobile databases which contain the confidential enterprise data, are the most common hacker attacks on mobile phones Qian et al. [41]. Notwithstanding, there will be a time when personal computers would become mobile phones Want et al. [40]. Small smart phone companies have entered into the technological market of today. To simplify, these new smart phones come pre-installed with Linux Ubuntu Touch and are significant during an investigation of a crime in terms of forensic evidence while, they also pose as a challenge for forensic investigators. Pine64 can be seen as one example of these smart phones Keim et al. [42].

5.3. Docker Updates and Unpatched Software

According to the authors of research paper Jain et al. [43], log files have been the norm when monitoring activities on a computer network. Furthermore, the concept of having a log system which is centralised by default and would allow an administrator to monitor regularly basis Jain et al. [43]. On top of that, referring to the reviews of the authors of the research paper Jain et al. [43], there are bound to be unique vulnerabilities in Docker images because, of their association with different programs and this can lead to various threats to a computer network. In addition, data leaks could occur while, tackling the different types of security holes that have occurred. To put it another way, Docker has no regard to sort out and fix bugs that, have been found in Docker images Jain et al. [43].

Furthermore, users could learn and teach other users on how to build their own Docker images from the beginning to the end with a Dockerfile Doan et al. [44], Wu et al. [45]. What is more, this will evaluate the secure framework with the use case where users will have frequent access to data in order to closely give real world scenarios Santos et al. [13]. According to the authors of these research paper Leahy et al. [46], Bettini et al. [47], Sultan et al. [48], Wist et al. [49], Doan et al. [44] and their concern about the potential security risks of Docker images and Docker containers on the other hand, in 2017 the authors of research paper Lu et al. [50] also expressed concerns relating to the security of Docker containers used in the cloud space especially since Docker containers where now gaining in popularity and compared to the traditional virtualisation for instance, VirtualBox and VMware Lu et al.[50].

On the second hand, on 31.8.2021 the CEO Scott Johnston of Docker elaborated on these researchers concerns. Docker Updates Product Subscriptions to Deliver Speed, Scale and Security. To further understand the role of Docker in relations to security, on 10.05.2022 the CEO Scott Johnston mentioned the purchase of Docker Accelerates Investment in Container Security with Acquisition of Nestybox which would add more security to Docker containers.

Meanwhile, on 21.07.2022 the CEO Scott Johnston of Docker said the security teams and developers would decrease the vulnerability of Docker software and at the same time ship Docker software at a faster rate. Docker Acquisition of Atomist Helps Meet Challenge of Securing Software Supply Chains for Development Teams. Evidently, it shows that Docker leadership and board of directors, take security very seriously with regards to Docker software, Docker images and Docker containers. An up to date information on Docker can be found at the following Docker blog website.

6. Putting Profit Ahead of Security

Referring to the views of the authors of research paper Jain et al. [43], centralisation and CaaS (Containers as a Service) are part of what would make Docker containers become more secure in a cloud Internet environment meanwhile, this is disingenuous at best. To put it another way, the authors of the research paper Jain et al. [43] deliberately forgot to mention that CaaS (Containers as a Service) is monetised but, gave examples of companies such as, Google (Google CloudRun), Amazon (AWS Fargate) and Microsoft (Azure Container Instances) which, use CaaS (Containers as a Service) Jain et al. [43]. A serious weakness with this argument however, is that the authors of research paper Alwabel et al. [51] are not alone saying that, money + security = (equals too) the security of users data and the database hosting the data on the other hand, the authors of research paper Patra et al. [52], Turuk et al. [53], Patra et al.[54] also supports a pay-as-you-go cloud-based service within the cloud Internet Patra et al. [52], Turuk et al. [53], Patra et al.[54].

Considering, in October 2001 Microsoft released Windows XP while, the last and final release was 2008. On 08.04.2014, was the date security updates and the support of Windows XP ended. Additionally, the National Health Service (NHS) suffered a ransomware attack called WannaCry which, prompted Microsoft to release a patch in 2017. Furthermore, a reality check happened while the National Health Service (NHS) were migrating their computer hardware from Windows XP to Windows 7 and Windows 10, problems of compatibility issues among the hardware, software and the financial aspect of upgrading to new hardware combined with the cost of the new operating system, software applications and the engineers cost Are old operating systems putting the NHS at risk in

2020?. To clarify, the author of research paper Odowd et al. [55] explained how WannaCry ransomware would encrypt all the files on the computer, lockout the owner from his or her own computer and then threaten the owner of such computer that to get access to the data on their computer, they would need to pay a ransom. Some of the affected hospitals in the United Kingdom (UK) were United Lincolnshire Hospitals NHS, University Hospitals of North Midlands NHS and Barts Health NHS Trust in London Odowd et al.[55]. Moreover, WannaCry ransomware hit over 150 countries and affected between one hundred thousand - four hundred thousand computers Aljaidi et al. [56], Odowd et al. [55].

In other words, the web page What is CaaS (Containers as a Service)? says, companies or industries can manage their container, clusters and applications which are virtualised by, getting them deployed easier and faster. In addition to, a pay-as-you-go cloud-based service is what CaaS (Containers as a Service) is. Moreover, the web page What is CaaS (Containers as a Service)? offers a reduced price to pay for only what you have used in relation to their services. To exemplify, computer instances, scheduling and balancing while, operating costs, infrastructure and software licensing can be reduced What is CaaS (Containers as a Service)? . Another line of thought on, container as a service (CaaS) that obviously is all about how much money providers of this service can make and the idea that money associated with security means, that the databases belonging to industries, academic institutions, banks, hospitals, the private sectors, small businesses etc. that subscribe to this model, means that all their users credentials are safe from internal or external attacks by hackers and intruders who do not have the right to access these databases Alwabel et al. [51].

According to the authors of research paper Said et al. [3], Huijie et al. [28],Wagner et al. [2], Elem et al. [27] and especially Internet websites like, Meta hit with record $1.3bn fine for its handling of EU user data, STEAM, Sony Data Breaches: Full Timeline Through 2023 and Recent Data Breaches – 2023 that have the current news on databases that have been breached or hacked recently, one major drawback to this approach is that, money + security $\neq$ (does not equal too) the security of users data and the database hosting the data Alwabel et al. [51]. To begin with, on 14.03.2023 users who had an organisation account on Docker Hub were told to upgrade their account or risk losing the account. Another thing to remember, this upgrade would come at a cost of $420 a year and paid monthly. Open source communities mostly use these type of accounts Docker is deleting Open Source organisations - what you need to know but, on 24.03.2023 Docker reversed its decision and apologised to all concerned We apologize. We did a terrible job announcing the end of Docker Free Teams.. More information can be found on the Frequently Asked Questions (FAQ) webpage As of March 24, 2023, Docker has reversed its decision to sunset the "Docker Free Team" plan. Read on for details.

Lastly, Meta must stop collecting the European Unions (EU) data, then sending it to the United States (US) and must also pay a massive fine of $1.3 billion. Meta hit with record $1.3 billion fine for its handling of EU user data. In light of, what happened this year (May 2023) to SONY PICTURES and the effect it caused to 6,791 former and current employees, having been told their data had being stolen by hackers. Additionally, the trend of keep data centralised on one database, will always be a problem and easy target for hackers Sony Data Breaches: Full Timeline Through 2023 Wagner et al. [2]. Hence, an up to date regarding information on database insecurity from January 2023 - to-date can be found on this webpage Recent Data Breaches - 2023. Considering, the events that occurred last month (October 2023) at STEAM where a hacker managed to gain access to the accounts of some developers on the STEAM platform. Furthermore, these accounts were used to spread malware in the form of, presenting them as legitimate updates for the games hosted on the platform which, some users of the platform downloaded as an update for their games. In other words, between 1 to 100 users downloaded this malware. In conclusion, STEAM has implemented a two step authentication for their developers to prevent this happening in future Steam Store Spreads Malware After Hacker Hijacks Developer Accounts.

7. Data Collection from Two Different Databases Hosted on the Internet

In this research we installed the free open-source software of both Damn Vulnerable Web Application (DVWA) database and database in a Docker engine: The authors of the research papers Tyagi et al. [57], Costa et al. [58], Makino et al. [59] employed Damn Vulnerable Web Application (DVWA) in their research while, the authors of the research papers Nagpure et al. [60] and Vyamajala et al. [61] used Acunetix their research.

7.1. Measuring Instruments - Psychometrics - Glances

These two researchers, Manore et al. [62] and Kok et .al [63] have successfully used Glances during their respective research. Glances is written in Python and is a system monitoring tool. It can be downloaded from Glances. Glances will be used to measure the metrics (CPU, data throughput, memory and time). Depending on the terminal size glances can adapt dynamically. It works in a web interface, via the Linux terminal remote monitoring could be done and can also work in a client/server mode. The readings of the metrics (CPU, data throughput memory and time) are saved in real-time to a CSV (Comma-Separated Values) file which in turn can be opened in LibreOffice Calc and read. Glances is shared under the LGPL version 3 license GNU LESSER GENERAL PUBLIC LICENSE.

8. Performance Data and Trade Off Results

Primarily, Figures 3–6 represent the performance data of the CPU (Central Processing Unit) while, Figures 7–10 represent the performance data of the memory. Furthermore, Figures 3–6 represent the performance data of the CPU (Central Processing Unit) while, Figures 7–10 represent the performance data of the memory. On the other hand, based of the charts the trade off between Acunetix with Docker CPU Performance Data Figure 3 and DVWA with Docker CPU Performance Data 5 is performance, the CPU of both Acunetix with Docker CPU Performance Data figure 3 and DVWA with Docker CPU Performance Data 5 reading are mostly between 35% - 100% while, going down to between 5% - 10% later on. Besides, figure Acunetix no Docker CPU Performance Data 4 and figure DVWA no Docker CPU Performance Data 6 a percentage of between 1% - 38% as evidence, this shows that Docker does not improve the performance of a database but improves the security of a database, the trade off here is the performance of the database but, at the expense of a secure database Ajasa et al. [64]. Despite this, the performance of Docker can be improved with the introduction and use of the video card Nvidia - (GPU - Graphics Processing Unit) in databases Choquette et al. [65].

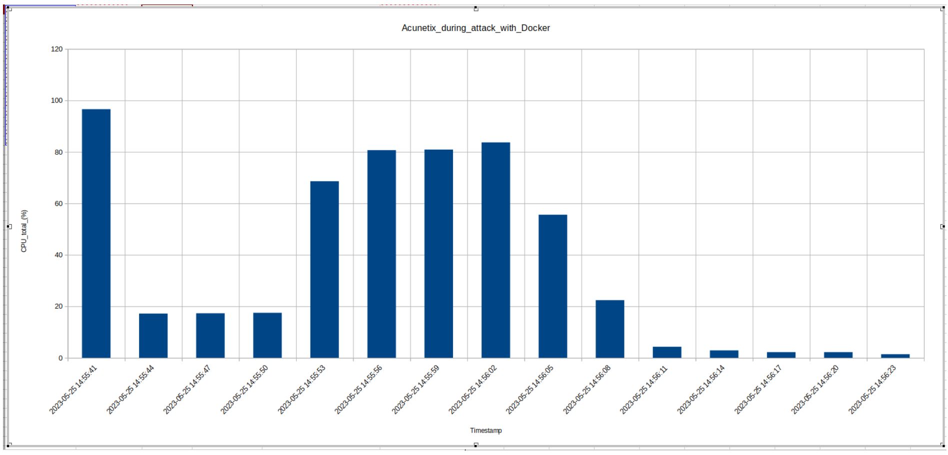

Figure 3. Acunetix with Docker CPU Performance Data.

doi:10.20944/preprints202507.1379.v1

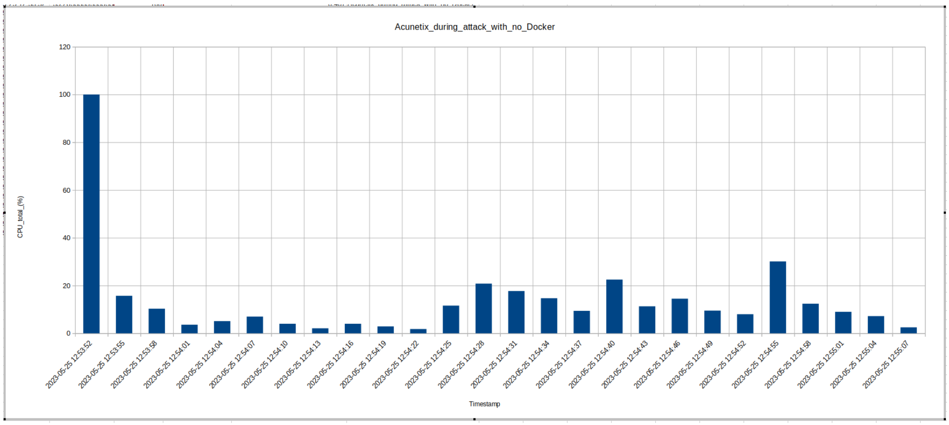

Figure 4. Acunetix no Docker CPU Performance Data.

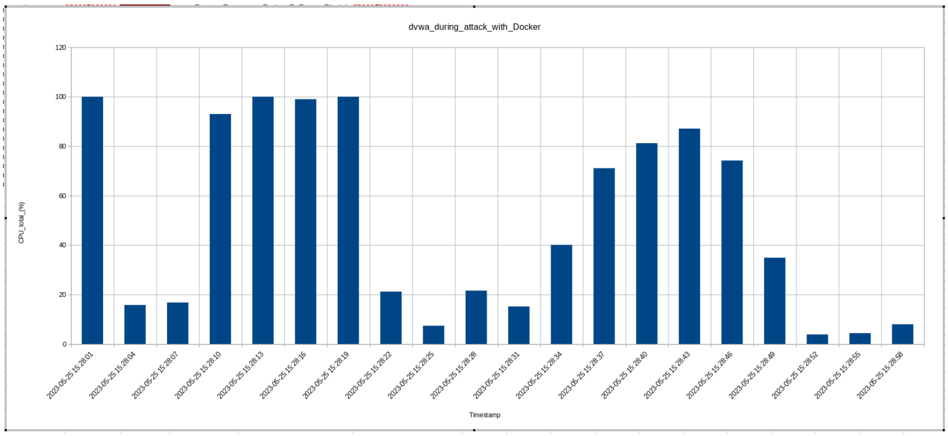

Figure 5. DVWA with Docker CPU Performance Data.

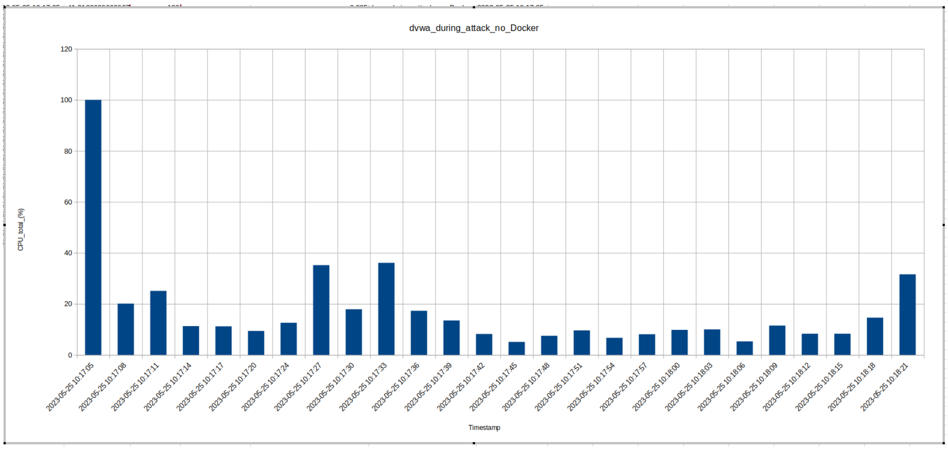

Figure 6. DVWA no Docker CPU Performance Data.

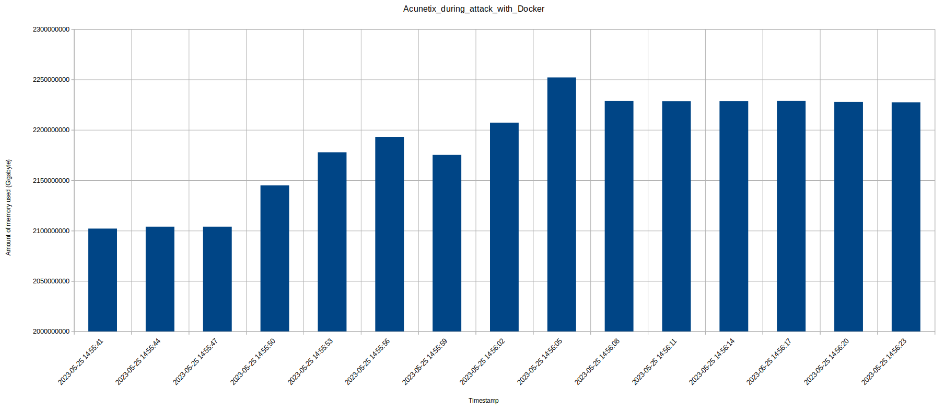

Figure 7. Acunetix With Docker Memory Performance Data.

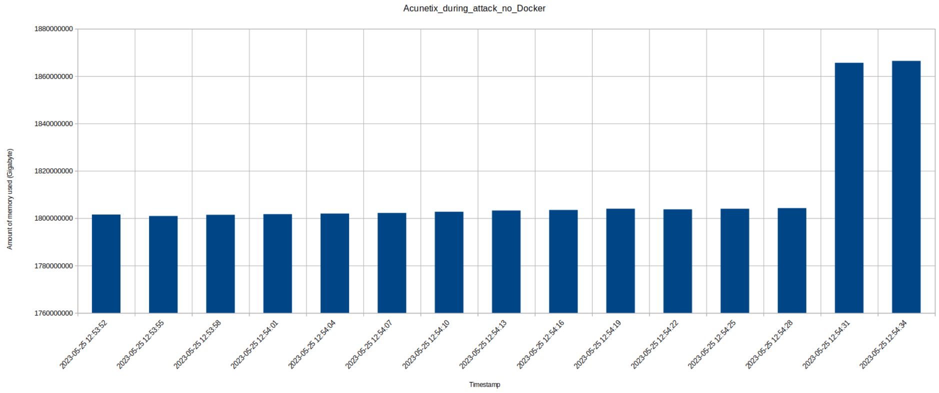

Figure 8. Acunetix no Docker Memory Performance Data.

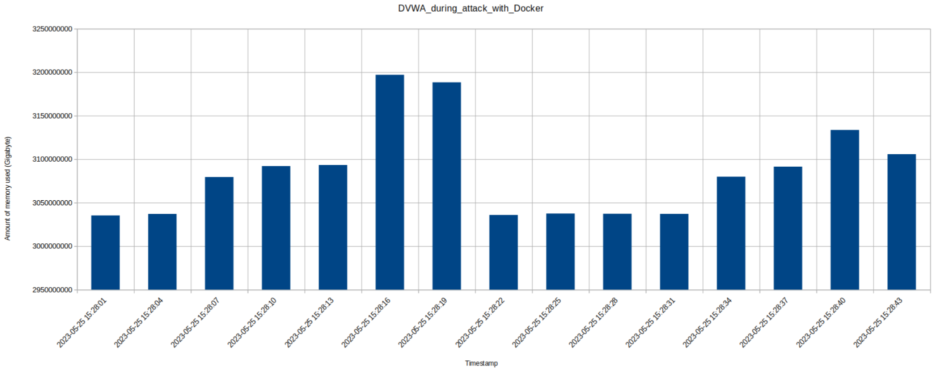

Figure 9. DVWA with Docker Memory Performance Data.

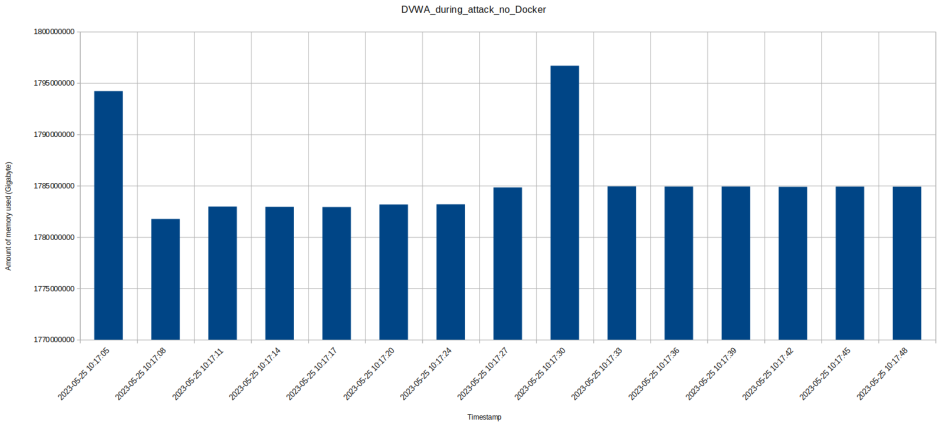

Figure 10. DVWA no Docker Memory Performance Data.

On the second hand, the figure of Acunetix with Docker Memory Performance Data 7 uses more memory than figure DVWA with Docker Memory Performance Data 9 but, the memory used by figure DVWA with Docker Memory Performance Data 9 is also a lot. Whereas, the memory used by figures Acunetix no Docker Memory Performance Data 8 and figures DVWA no Docker Memory Performance Data 10 are less compared to figures Acunetix with Docker Memory Performance Data 7 and DVWA with Docker Memory Performance Data 9 meanwhile, the trade off we have here is that when Docker is employed with a databases more, memory is needed and the trade off here is that Docker consumes a lot of memory when used with a database compared to when it is not used with a database Singh et al. [66].

8.1. Performance Data - CPU

Acunetix and DVWA performance data - central processing unit.

8.2. Performance Data - Memory

Acunetix and DVWA performance data - memory.

9. Summary of Findings

Meanwhile, the authors of the research paper Gore et al. [67] had a positive result when utilising Docker containers handling data in a network environment compared to the results of the authors of the research paper Velasquez el al. [68] that showed Microsoft Azure, Amazon Web Services, OpenStack, IBM, VMware and Google Compute Engine which, are all cloud providers are now been supported by Docker. Additionally, the authors of the research paper Reis et al. [69] developers are not keen on using different types of tools to build their Docker-compose.yml files and Dockerfiles. According to the author of the research paper Alkhimenkov et al. [70], the GPU (General Processing Unit) can increase the performance and execution time of application Alkhimenkov et al. [70]. Furthermore authors of the research paper Choquette et al. [65] said, programming model design and system integration, transistors are the contribution that a lot engineers have contributed to NVIDIA GPUs. The GPU has increased the speed were cloud computing is used especially were data centres are concerned. Scientific computing, data analytics, cloud gaming, inference (taking steps to reason logically) and AI deep learning training, 5G services, genomics (genetics), graphics rendering and video analytics are examples of the applications benefiting from a GPU Choquette et al. [65].

On top of that, the difference in the architecture of both the CPU (Central Processing Unit) and GPU processing units is that, similar to what authors of the research paper Choquette et al. [65] said, the GPU geared towards performance, rendering and (3D) modelling. While. the CPU handles the scheduling operations, computing, data transfer etc. The GPU is an extremely powerful computer processor especially when been used with virtualisation, intensive applications and the processing of data Castano et al. [71]. The authors of the research paper Saha et al. [72] suggested that there should be a demonstration from a single laptop that, Docker works automatically and seamlessly. On top of that, to avoid the failure of one or more services there has to be a conduct performance test which, should be conducted to see how long it would take the system to recover. Additionally, there is zero service disruption guarantees i.e the system is capable of withstanding injected failures Saha et al. [72]. On the other hand, the authors of the research paper Aleksandrovs et al. [73] in their findings of the simulation concluded that it is good to apply Docker containers when you need a faster architecture Aleksandrovs et al. [73].

According to the researchers of the research paper Seifi et al.[74], found everywhere in modern computing systems as accelerators are GPUs which, can deliver unusually huge processing capabilities. GPUs are used with graphics, artificial intelligence, scientific computing, mobile devices and cloud servers Seifi et al. [74].

10. Conclusions

Firstly, the decentralised nature of this approach empowers users with greater control over their data, improving accessibility and reducing the risk of unauthorised access. The findings of this research suggest that a Docker-based database can provide a robust and secure solution for various applications. By isolating database instances within containers this not only improves security but, allows the user to quickly find out where the problem has occurred within the container were the database is operating from. In addition, most if not all data breaches have originated from a centralised database, which is a weak point the hackers could easily attack or circumvent. Moreover, a decentralised database is far more secure than the traditional centralised database, the most important thing to secure is the users data, the database hosting the users data, the consensus between users and the authority or government in charge of the database.

References

1. Zhao, X.; Lin, Q.; Chen, J.; Wang, X.; Yu, J.; Ming, Z. Optimizing security and quality of service in a Real-time database system using Multi-objective genetic algorithm **2016**. *64*, 11–23.
2. Wagner, J.; Rasin, A.; Glavic, B.; Heart, K.; Furst, J.; Bressan, L.; Grier, J. Carving database storage to detect and trace security breaches **2017**. *22*, S127–S136. https://doi.org/10.1016/j.diin.2017.06.006.
3. Said, W.; Mostafa, A.M. Towards a Hybrid Immune Algorithm Based on Danger Theory for Database Security **2020**. *8*, 145332–145362. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2020.3015399.
4. Tahir, M.; Abdullah, A.; Udzir, N.I.; Kasmiran, K.A. A novel approach for handling missing data to enhance network intrusion detection system **2024**. *3*, 100063. https://doi.org/10.1016/j.csa.2024.100063.
5. Neto, N.N.; Madnick, S.; Paula, A.M.G.D.; Borges, N.M. Developing a Global Data Breach Database and the Challenges Encountered. *Journal of Data and Information Quality* **2021**, *13*, 1–33. https://doi.org/10.1145/3439873.
6. Algarni, A.M.; Thayananthan, V.; Malaiya, Y.K. Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences* **2021**, *11*, 3678. Number: 8 Publisher: Multidisciplinary Digital Publishing Institute, https://doi.org/10.3390/app11083678.
7. Wang, K.C.; Reiter, M.K. Using Amnesia to Detect Credential Database Breaches **2021**. p. 18.
8. Hassanzadeh, Z.; Biddle, R.; Marsen, S. User Perception of Data Breaches. *IEEE Transactions on Professional Communication* **2021**, *64*, 374–389. Conference Name: IEEE Transactions on Professional Communication, https://doi.org/10.1109/TPC.2021.3110545.
9. Goel, K.; Hofstede, A.H.M.T. Privacy-Breaching Patterns in NoSQL Databases. *IEEE Access* **2021**, *9*, 35229–35239. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2021.3062034.
10. Miyamoto, E. The Decades-Long Struggle of 'Comfort Women' for Justice **2023**. *6*, 272–278. Number: 1, https://doi.org/10.34190/icgr.6.1.1103.
11. Seidelman, W.E. Nuremberg lamentation: for the forgotten victims of medical science. *BMJ : British Medical Journal* **1996**, *313*, 1463–1467.
12. Zaw, T.M.; Thant, M.; Bezzateev, S. Database Security with AES Encryption, Elliptic Curve Encryption and Signature. In Proceedings of the 2019 Wave Electronics and Its Application in Information and Telecommunication Systems (weconf), New York, 2019. WOS:000635354100017.

13. Santos, N.; Younis, W.; Ghita, B.; Masala, G. Enhancing Medical Data Security on Public Cloud. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 103–108. https://doi.org/10.1109/CSR51186.2021.9527987.
14. Crooks, N. A Client-centric Approach to Transactional Datastores. In Proceedings of the Proceedings of the 2021 International Conference on Management of Data. ACM, 2021, pp. 3–5. https://doi.org/10.1145/3448016.3461471.
15. Toapanta, S.M.T.; Gallegos, L.E.M.; Trejo, J.A.O. Security analysis of civil registry database of Ecuador. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). IEEE, 2016, pp. 1024–1029. https://doi.org/10.1109/ICEEOT.2016.7754841.
16. Perri, D.; Simonetti, M.; Gervasi, O. Deploying Efficiently Modern Applications on Cloud. *Electronics* **2022**, *11*, 450. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute, https://doi.org/10.3390/electronics11030450.
17. Nelson Novaes Neto.; Stuart Madnick.; Anchises Moraes G. de Paula.; Natasha Malara Borges. Cyber Security Data Breaches, 2022.
18. Ding, Y.; Sato, H. Dagbase: A Decentralized Database Platform Using DAG-Based Consensus. In Proceedings of the 2020 Ieee 44th Annual Computers, Software, and Applications Conference (compsac 2020); Chan, W.K.; Claycomb, B.; Takakura, H.; Yang, J.J.; Teranishi, Y.; Towey, D.; Segura, S.; Shahriar, H.; Reisman, S.; Ahamed, S.I., Eds., New York, 2020; pp. 798–807. ISSN: 0730-3157 WOS:000629086600105, https://doi.org/10.1109/COMPSAC48688.2020.0-164.
19. Samaraweera, G.D.; Chang, J.M. Security and Privacy Implications on Database Systems in Big Data Era: A Survey **2021**. *33*, 239–258. Conference Name: IEEE Transactions on Knowledge and Data Engineering, https://doi.org/10.1109/TKDE.2019.2929794.
20. Nash, T.; Olmsted, A. Performance vs. security: Implementing an immutable database in MySQL. In Proceedings of the 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2017, pp. 290–291. https://doi.org/10.23919/ICITST.2017.8356402.
21. Lee, B.H.; Dewi, E.K.; Wajdi, M.F. Data Security in Cloud Computing Using AES Under HEROKU Cloud. In Proceedings of the 2018 27th Wireless and Optical Communication Conference (wocc), New York, 2018; pp. 242–246. ISSN: 2379-1268 WOS:000443454700060.
22. Odirichukwu, J.C.; Asagba, P.O. Security concept in web database development and administration — A review perspective. In Proceedings of the 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), 2017, pp. 383–391. ISSN: 2377-2697, https://doi.org/10.1109/NIGERCON.2017.8281910.
23. Deepa, G.; Thilagam, P.S. Securing web applications from injection and logic vulnerabilities **2016**. *74*, 160–180. https://doi.org/10.1016/j.infsof.2016.02.005.
24. Park, J.H.; Yoo, S.M.; Kim, I.S.; Lee, D.H. Security Architecture for a Secure Database on Android. *Ieee Access* **2018**, *6*, 11482–11501. Place: Piscataway Publisher: Ieee-Inst Electrical Electronics Engineers Inc WOS:000622030100002, https://doi.org/10.1109/ACCESS.2018.2799384.
25. Gao, B. Path Analysis of Using Big Data to Build Engineering Cost Database under the Background of Information Management. In Proceedings of the 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). IEEE, 2020, pp. 1963–1966. https://doi.org/10.1109/ICMCCE51767.2020.00430.
26. Khan, W.; Ahmad, W.; Luo, B.; Ahmed, E. SQL Database with physical database tuning technique and NoSQL graph database comparisons. In Proceedings of the Proceedings of 2019 Ieee 3rd Information Technology, Networking, Electronic and Automation Control Conference (itnec 2019); Xu, B., Ed., New York, 2019; pp. 110–116. WOS:000491352900022.
27. Elem, M.; Elem, N.; Obinna, C. Online Database Security Threats and Solutions: The NetFlix Incident **2020**. *5*, 6.
28. Huijie, W. A Security Framework for Database Auditing System. In Proceedings of the 2017 10th International Symposium on Computational Intelligence and Design (iscid), Vol. 1, New York, 2017; pp. 350–353. ISSN: 2165-1701 WOS:000427991100080, https://doi.org/10.1109/ISCID.2017.64.
29. Jusak, J.; Mahmoud, S.S.; Laurens, R.; Alsulami, M.; Fang, Q. A New Approach for Secure Cloud-Based Electronic Health Record and its Experimental Testbed. *IEEE Access* **2022**, *10*, 1082–1095. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2021.3138135.

30. Kalkman, S.; van Delden, J.; Banerjee, A.; Tyl, B.; Mostert, M.; van Thiel, G. Patients' and public views and attitudes towards the sharing of health data for research: a narrative review of the empirical evidence. *Journal of Medical Ethics* **2022**, *48*, 3–13. https://doi.org/10.1136/medethics-2019-105651.
31. He, Y.; Maglaras, L.; Aliyu, A.; Luo, C. Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure **2022**. *2022*, 1–10. https://doi.org/10.1155/2022/2775249.
32. Khan, S.; Kabanov, I.; Hua, Y.; Madnick, S. A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned **2023**. *26*, 1–29. https://doi.org/10.1145/3546068.
33. Liu, J.; Ni, X. Ordeal by innocence in the big-data era: Intended data breach disclosure, unintended real activities manipulation **2023**. *n/a*. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/eufm.12410, https://doi.org/10.1111/eufm.12410.
34. Li, Y.; Mamon, R. Modelling health-data breaches with application to cyber insurance **2023**. *124*, 102963. https://doi.org/10.1016/j.cose.2022.102963.
35. Vinicius, L.; Rodrigues, L.; Torquato, M.; Silva, F.A. Docker platform aging: a systematic performance evaluation and prediction of resource consumption **2022**. *78*, 1–31. https://doi.org/10.1007/s11227-022-04389-4.
36. Ahmed, A.; Pierre, G. Docker Image Sharing in Distributed Fog Infrastructures. In Proceedings of the 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2019, pp. 135–142. ISSN: 2330-2186, https://doi.org/10.1109/CloudCom.2019.00030.
37. Rad, B.B.; Bhatti, H.J.; Ahmadi, M. An Introduction to Docker and Analysis of its Performance. *International Journal of Computer Science and Network Security* **2017**, *17*, 228–235. Place: Seoul Publisher: Int Journal Computer Science & Network Security-Ijcsns WOS:000402797500027.
38. Pratap Yadav, M.; Pal, N.; Kumar Yadav, D. A formal approach for Docker container deployment. *Concurrency and Computation: Practice and Experience* **2021**, *33*. https://doi.org/10.1002/cpe.6364.
39. Musleh, S.; Islam, M.T.; Qureshi, R.; Alajez, N.M.; Alam, T. MSLP: mRNA subcellular localization predictor based on machine learning techniques **2023**. *24*, 109. https://doi.org/10.1186/s12859-023-05232-0.
40. Want, R. When Cell Phones Become Computers **2009**. *8*, 2–5. Conference Name: IEEE Pervasive Computing, https://doi.org/10.1109/MPRV.2009.40.
41. Qian, K.; Lo, D.; Shahriar, H.; Li, L.; Wu, F.; Bhattacharya, P. Learning Database Security with Hands-on Mobile Labs. In Proceedings of the 2017 Ieee Frontiers in Education Conference (fie), New York, 2017. ISSN: 0190-5848 WOS:000426974900282.
42. Keim, Y.; Yoon, Y.H.; Karabiyik, U. Digital Forensics Analysis of Ubuntu Touch on PinePhone **2021**. *10*, 343. https://doi.org/10.3390/electronics10030343.
43. Jain, V.; Singh, B.; Choudhary, N.; Yadav, P.K. A Hybrid Model for Real-Time Docker Container Threat Detection and Vulnerability Analysis **2023**. *11*, 782–793. Number: 6s.
44. Doan, P.; Jung, S. DAVS: Dockerfile Analysis for Container Image Vulnerability Scanning **2022**. *72*, 1699–1711. https://doi.org/10.32604/cmc.2022.025096.
45. Wu, Y.; Zhang, Y.; Wang, T.; Wang, H. Dockerfile Changes in Practice: A Large-Scale Empirical Study of 4,110 Projects on GitHub. In Proceedings of the 2020 27th Asia-Pacific Software Engineering Conference (APSEC), 2020, pp. 247–256. ISSN: 2640-0715, https://doi.org/10.1109/APSEC51365.2020.00033.
46. Leahy, D.; Thorpe, C. Zero Trust Container Architecture (ZTCA): A Framework for Applying Zero Trust Principals to Docker Containers. *International Conference on Cyber Warfare and Security* **2022**, *17*, 111–120. Number: 1, https://doi.org/10.34190/iccws.17.1.35.
47. Bettini, A.; Com, F. VULNERABILITY EXPLOITATION IN DOCKER CONTAINER ENVIRONMENTS **2015**.
48. Sultan, S.; Ahmad, I.; Dimitriou, T. Container Security: Issues, Challenges, and the Road Ahead **2019**. *7*, 52976–52996. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2019.2911732.
49. Wist, K.; Helsem, M.; Gligoroski, D. Vulnerability Analysis of 2500 Docker Hub Images, 2020, [2006.02932 [cs]].
50. Lu, T.; Chen, J. Research of Penetration Testing Technology in Docker Environment. Atlantis Press, 2017, pp. 1354–1359. ISSN: 2352-5401, https://doi.org/10.2991/icmmcce-17.2017.238.
51. Alwabel, A. A Novel Container Placement Mechanism Based on Whale Optimization Algorithm for CaaS Clouds **2023**. *12*, 3369. Number: 15 Publisher: Multidisciplinary Digital Publishing Institute, https://doi.org/10.3390/electronics12153369.
52. Patra, M.K.; Sahoo, B.; Turuk, A.K.; Misra, S. Task grouping and optimized deep learning based VM sizing for hosting containers as a service **2023**. *12*, 65. https://doi.org/10.1186/s13677-023-00441-7.

53. Turuk, Bibhudatta Sahoo, A.K.M.K.P. Container as a Service in the Cloud: An Approach to Secure Hybrid Virtualization. In *Recent Trends and Best Practices in Industry 4.0*; River Publishers, 2023. Num Pages: 18.
54. Patra, M.K.; Misra, S.; Sahoo, B.; Turuk, A.K. GWO-Based Simulated Annealing Approach for Load Balancing in Cloud for Hosting Container as a Service **2022**. *12*, 11115. Number: 21 Publisher: Multidisciplinary Digital Publishing Institute, https://doi.org/10.3390/app122111115.
55. O'Dowd, A. Labour calls for inquiry into NHS cyber-attack **2017**. *357*, j2395. Publisher: British Medical Journal Publishing Group Section: News, https://doi.org/10.1136/bmj.j2395.
56. Aljaidi, M.; Alsarhan, A.; Samara, G.; Alazaidah, R.; Almatarneh, S.; Khalid, M.; Al-Gumaei, Y.A. NHS WannaCry Ransomware Attack: Technical Explanation of The Vulnerability, Exploitation, and Countermeasures. In Proceedings of the 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), 2022, pp. 1–6. https://doi.org/10.1109/EICEEAI56378.2022.10050485.
57. Tyagi, S.; Kumar, K. Evaluation of Static Web Vulnerability Analysis Tools. In Proceedings of the 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE, 2018, pp. 1–6. https://doi.org/10.1109/PDGC.2018.8745996.
58. Costa, G.; Russo, E.; Valenza, A. Damn Vulnerable Application Scanner **2021**. p. 15.
59. Makino, Y.; Klyuev, V. Evaluation of web vulnerability scanners. In Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE, 2015, pp. 399–402. https://doi.org/10.1109/IDAACS.2015.7340766.
60. Nagpure, S.; Kurkure, S. Vulnerability Assessment and Penetration Testing of Web Application. In Proceedings of the 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). IEEE, 2017, pp. 1–6. https://doi.org/10.1109/ICCUBEA.2017.8463920.
61. Vyamajala, S.; Mohd, T.K.; Javaid, A. A Real-World Implementation of SQL Injection Attack Using Open Source Tools for Enhanced Cybersecurity Learning. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT). IEEE, 2018, pp. 0198–0202. https://doi.org/10.1109/EIT.2018.8500136.
62. Manore, C.; Manjunath, P.; Larkin, D. Performance of Single Board Computers for Vision Processing. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2021, pp. 0883–0889. https://doi.org/10.1109/CCWC51732.2021.9376035.
63. Kok, G.X.; Choong, K.N.; Vethanayagam, C.; Owada, Y.; Sato, G. An Analysis of a Large Scale Wireless Image Distribution System Deployment. In Proceedings of the 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE, 2019, pp. 150–155. https://doi.org/10.1109/ISCAIE.2019.8743734.
64. Ajasa, A.D.; Chizari, H.; Alam, A. Database Security and Performance: A Case of SQL Injection Attacks Using Docker-Based Virtualisation and Its Effect on Performance. *Future Internet* **2025**, *17*, 156. Number: 4 Publisher: Multidisciplinary Digital Publishing Institute, https://doi.org/10.3390/fi17040156.
65. Choquette, J.; Gandhi, W.; Giroux, O.; Stam, N.; Krashinsky, R. NVIDIA A100 Tensor Core GPU: Performance and Innovation. *IEEE Micro* **2021**, *41*, 29–35. Conference Name: IEEE Micro, https://doi.org/10.1109/MM.2021.3061394.
66. Singh, N.; Hamid, Y.; Juneja, S.; Srivastava, G.; Dhiman, G.; Gadekallu, T.R.; Shah, M.A. Load balancing and service discovery using Docker Swarm for microservice based big data applications **2023**. *12*, 4. https://doi.org/10.1186/s13677-022-00358-7.
67. Gore, R.; Banerjea, S.; Tyagi, N.; Saurav, S.; Acharya, D.; Verma, V. An Efficient Edge Analytical Model on Docker Containers for Automated Monitoring of Public Restrooms in India. In Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2020, pp. 1–6. https://doi.org/10.1109/ANTS50601.2020.9342845.
68. Velasquez, W.; Munoz-Arcentales, A.; Salvachua Rodriguez, J. A Case Study: Ingestion Analysis of WSN Data in Databases using Docker. In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (iccais' 2018), New York, 2018. WOS:000493071300040.
69. Reis, D.; Piedade, B.; Correia, F.F.; Dias, J.P.; Aguiar, A. Developing Docker and Docker-Compose Specifications: A Developers' Survey. *IEEE Access* **2022**, *10*, 2318–2329. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2021.3137671.
70. Alkhimenkov, Y. Digital rock physics: Calculation of effective elastic properties of heterogeneous materials using graphical processing units (GPUs). *Computers & Geosciences* **2025**, *194*, 105749. https://doi.org/10.1016/j.cageo.2024.105749.

71. Castaño-Díez, D.; Moser, D.; Schoenegger, A.; Pruggnaller, S.; Frangakis, A.S. Performance evaluation of image processing algorithms on the GPU. *Journal of Structural Biology* **2008**, *164*, 153–160. https://doi.org/10.1016/j.jsb.2008.07.006.
72. Saha, P.; Govindaraju, M.; Marru, S.; Pierce, M. Integrating Apache Airavata with Docker, Marathon, and Mesos **2016**. *28*, 1952–1959. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.3708, https://doi.org/10.1002/cpe.3708.
73. Aleksandrovs-Moisejs, D.; Ipatovs, A.; Grabs, E.; Rjazanovs, D. Evaluation of a Long-Distance IEEE 802.11ah Wireless Technology in Linux Using Docker Containers **2022**. *28*, 71–77. Number: 3, https://doi.org/10.5755/j02.eie.31146.
74. Seifi, N.; Al-Mamun, A. Optimizing Memory Access Efficiency in CUDA Kernel via Data Layout Technique. *Journal of Computer and Communications* **2024**, *12*, 124–139. https://doi.org/10.4236/jcc.2024.125009.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.