ISSN No:-2456-2165

Design and Development of Cloud-Based Cyber Risk Assessment System for a Hybrid Data Center

Tinashe Blessing Chuwe, Mainford Mutandavari
Department of Information Technology,
Department of Software Engineering
Harare Institute of Technology University

Abstract:- Regardless of massive investment into complex and advanced computing infrastructure in Africa and Zimbabwe in particular, there is growing concern for the asymmetric development in comprehensive security systems to tally this thrust in technology investment. As Data Centres are deployed to solve complex industry and development problems in the country, the security infrastructure need to be considered as well by clearly applying identifiable cyber security risk management framework. This study therefore sought to:i.develop a cloud-based cyber security risk system to identify security vulnerabilities. ii estimate the Data centre aggregate risk score in real-time, and iii. Control identified threats. The results indicate that the proposed risk assessment framework is no like any of the surveyed past such frameworks but helps to complement such. It adds to the perspective of managing risks at hybrid data centres. Ability to capture the human perspectives through creation of comprehensive requirement. text files helps to capture not only the technical details of the threats but also considers the human perspectives enriching the way risk is calculated and defined. A hybrid data centres have no unique vulnerabilities and threats than other computing infrastructure. However, it seems some vulnerabilities and threats are more common for the data centres than other infrastructure. In this study, denial of service and malware are some of the threats which are peculiar to data centres. Furthermore, due to complexity in the mixture and combination of software and application suit at a data centre, the range of threats may not be predefined nor generalised from one centre to the other. Empirical testing and verification of these weaknesses need customised and personalised approach as indicated in this study. For a comprehensive risk assessment framework that does not capture computing-related threats and vulnerabilities, further research is pertinent that also captures the human perspectives and other security dimensions such as the physical and personal security issues at the data centre. Better future frameworks may need to incorporate not only the quantitative risk assessments but incorporate the qualitative elements to risk.

Keywords:- *Data Centre, Software, Risk Score, Vulnerabilities, Framework, Threat, Exploits, Security.*

I. INTRODUCTION

Zimbabwe is on a spree to invest in advanced and complex computing infrastructure such as the ZCHPC and increasing procurement of security risk technologies to protect the same. There is also growing notable outcry for establishment of comprehensive cyber security regulations and laws. However, cases of cyber security attacks have been on the increase raising questions on the adequacy of current efforts to reduce and manage such risks [1]. One of the key concerns raised to date has been the lack of clear security risk management framework adopted by the Centre. Without clearly identifying functional risk management framework for the Centre may continue to pose security risk for the investment infrastructure. Zimbabwe installed a high-performance computing infrastructure termed the Zimbabwe Centre for High Performance Computing (ZCHPC) in 2015 with the help of Inspur, a Chinese technology firm for purposes of driving economic growth of the country through advanced information communication technologies (ICTs) [1]. ZCHPC for example, located at the University of Zimbabwe campus, was meant to provide key solutions to contemporary problems: food security, poverty and diseases reduction, promote human capital and energy development, and advance research among others [2]. Since its inception the uptake of the technology has not been as expected with number of users not exceeding fifty by 2020[1]. The Centre offers both high performance computing resources and storage facilities to host huge volumes of data [3].

According to Mark[4], provisioning of data centres through a high performance computing environment renders the centre a high profile target for cyber security threats. While ZCHPC has been taunted as the hub for socio-economic development in Zimbabwe for instance, there is rising concern for security risks associated with such infrastructure [1]. Mtetwa [1] acknowledges that Zimbabwe has gained social and economic development enhanced by the emergence of information society especially spurred installation of vital information technology infrastructure such as the Zimbabwe Centre for High Performance Computing (ZCHPC). However, the author is quick to underscore the twin issue of increases in cyber security threats that may endanger the aforementioned gains. The author seems them to suggests that implementation of cyber security laws, cyber governance and investment in computer security coupled by international cooperation might help reduce such threats landscape. Furthermore, [5]propounds that data centres operating in a supercomputing environment may spot threats. This is also supported by [6] who highlight the numerous benefits of supercomputing environments without indicating the costs and emegernce of complex

ISSN No:-2456-2165

threats spurred by such infrastructure. However, these views seem to be only suggestive and not based on empirical evidence. Unfortunately, [7] and [3] demonstrate that a number of such Data Centres have been hacked across European countries in the recent past and are centres of cyber threat attack targets. This is echoed by [8] and [9] who reiterate that high performance computing environments inclusive of the associated data centres are most preferred targets for cyber threat attacks – targets for breach of confidientality, integrity and availability of such systems.

Exploring of literature seem to suggest that a number of such infrastructure are pursuing different security risk management frameworks such as the ISO 27002/ ISO 31000; National Institute of Standards and Technology (NIST) Cyber security Framework; and CIS Controls among others [10]. While indeed most of the frameworks have matured over the years, they lack to reflect cultural and contextual differences ([11];[9]). According to [11], the extant security frameworks are Western driven concepts and require adjustment and contextualisation in countries influenced by different cultures such as Africa and the Middle East regions. Against these realities, the researcher found it pertinent to apply the existing cybersecurity risk assessment frameworks particularly the ISO 27000/ISO 31000 to the identification of the potential cyber threats for Data centre and assess the adequacy of current risk controls to manage the identified threats and risks.

Adoption of clear cyber security risk management framework might complement current efforts in security infrastructure for the Centre and creation of the necessary cyber security policies and laws in Zimbabwe [1][2]. ZCHPC is aimed to be the hub of socio-economic development in Zimbabwe and the major driver of advanced research in Zimbabwe. It is therefore pertinent that improvement of the security posture of such Centres be implemented to realise such long-term goals. The benefits of computing infrastructure can hardly be isolated from its associated security requirements [7][10].

Some Data centres continue to invest in technology and security infrastructure without clearly applying identifiable cyber security risk management framework creating a continued gap in notable increases in cases of cyber security attacks and potential threat which may impede the achievement of the goals of the Data Centre.

Therefore, the purpose of this study is to develop a systematic cloud-based cyber security risk assessment system adaptive to different data centre architectures. Specifically, the research sought:

- To determine Data Centre's ways of detecting security threats.
- To identify the security vulnerabilities of the Data Centre
- To estimate the aggregate risk score for the Data Centre
- To identify the control measures implemented at the Data Centre to handle the identified security threats.

II. METHODOLOGY

The section presents the step-by-step procedure that was used to design, develop, test and validate the cloud-based cyber security risk assessment system for the Data centre that can provide an overall risk level for a hybrid data centre. This study adopted a system design methodology by clearly accounting for each require software and hardware requirements of the system. The proposed system does not only provide vulnerabilities and risks for individual software that may use at a hybrid data centre but also aggregates those into an overall risk score that may provide a better view of the security risks at such complex centres.

A. Materials

An HP Envy laptop with 8GB RAM; Core i5; 2.3 GHz Intel (R) and 1 Tera HDD running Ubuntu 18.04, and Django development platform. The developer made use of Python 3.7 to develop the web application needed for the system; and JQUERY for JavaScript programming. For database development and management, the developer relied on *Vulners* online database to host the system on cloud, and MYSQL for storage of the user and Internet data.

B. Design and Development of the System

The cyber risk assessment framework for a hybrid data centre was conceptualised as indicated in Figure 1.

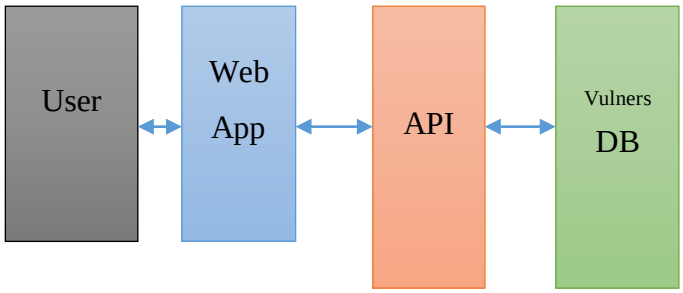

Fig. 1: Architecture of the risk assessment framework for a hybrid data centre

Source: Researcher 2021

The framework was designed in modular form covering functions for user login, module to add a file for scan, module to list information added, module to scan the contents input file one by one, module to list scan results, module to add CVE IDE for vulnerabilities, module to show the results and the risk score, and module to aggregate risk score. The modules were designed such that the user who would like to calculate the risk level measured as a risk score would need to login on the Web APP using the user credentials. The Web App has internal modules to add files, list information of files added, scan the contents of the files one by one and then produces scan results. Once this is completed, the Web App needs send the files to vulners.com website for vulnerability analysis. The module to add CVE IDE also has ability to calculate the risk scores for each software analysed and then aggregate these to come up with the overall risk score for the data centre.

C. Development

AT this stage the researcher had to develop the system as depicted in Figure 2.

ISSN No:-2456-2165

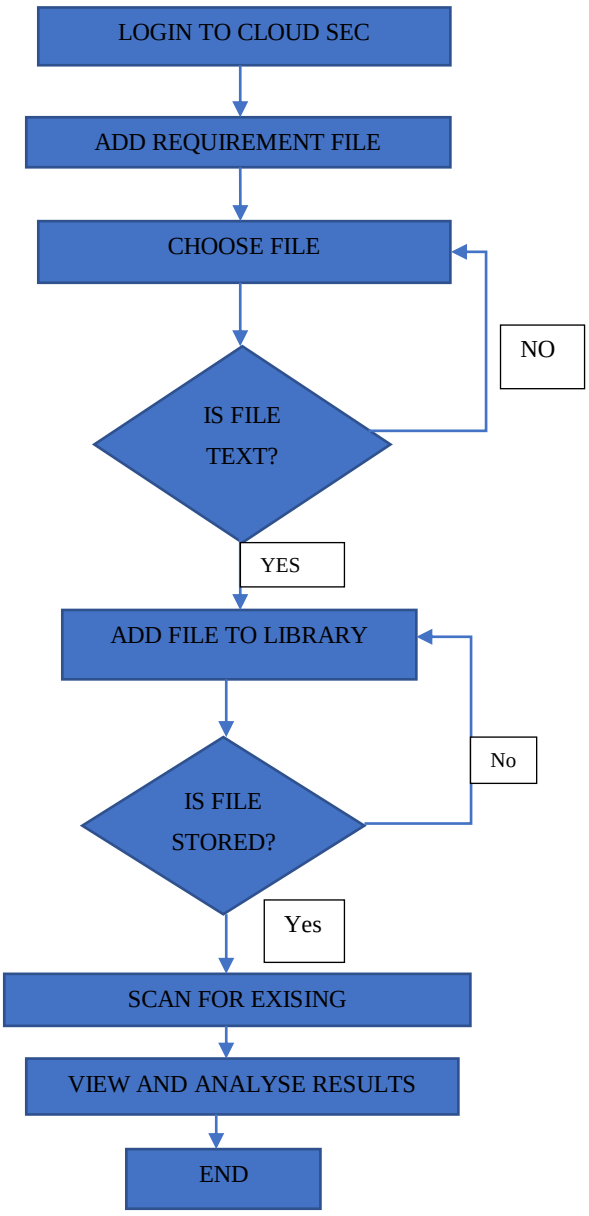

Fig. 2: Development algorithm for risk assessment framework for a hybrid data centre

Source: Researcher 2021

As shown in Figure 2, the researcher had to develop the web application (web app) which was used to login to the Vulners database. The web app also had capabilities to check files required by Vulners. The files had to be text files containing relevant fields of information. The web app first scanned these files for the content information and which it would output as list of contents. This step is necessary in analysis of vulnerabilities as it provides some level of analysis that may be done.

D. Testing

The system was successfully designed and developed. Processes to check for the performance of the system were done by way of analysing some existing applications and software being used at the ZCHPC for example, as already defined in preceding sections – listed in the requirement. text file. The listed software and applications were successfully added to library and scanned for vulnerabilities producing some notable exploitable vulnerabilities in the existing set of software and applications being used.

E. Validation

After the performance testing, the researcher intended to verify if the developed solution can indeed provide some authentic records and reports of software and application vulnerabilities. The researcher used some software and applications that contained some vulnerabilities already known and identified by independent analysts. The results of scanning for vulnerabilities using the developed system were compared with those of the known vulnerabilities. This was meant to check for accuracy and ability of the system to make proper predictions and identification of the vulnerabilities. The system indicated significant performance criteria that can be relied on to provide some overview picture of the vulnerabilities at the Centre with some degree of accuracy and speedy. It offered a dashboard that helps administrators easily estimate the risk score for the Centre at anytime and anywhere. A cloud-based risk assessment solution provides potential capability to detect and recommend some measures which may improve the competitiveness of the Data centre.

III. RESULTS

A. Potential methods of identifying security threats at the ZCHPC Data Centre

Detection of security threats has pre-occupied technologists since the invention of the telephone system. Wiretapping and eavesdropping are some of the old techniques cyber criminals have attempted to disrupt normal computing operations. One of the major strategies to detect such criminal activities has been to design and develop complex anti-intrusion detection systems some that depend on signatures. However, these depend largely of detection techniques that can only detect those threats with known databases and signatures. New threats are hardly detectable unless the system is updated with the right signatures. In this study, the detection of the threats was not a direct method as in common detection systems but through analysis of the vulnerabilities detected in the application and software being used. Understanding the exploits used by the enemy to attack offers a better way to detect the king of threats one may be exposed to. The vulnerability identified was also listed together with possible cyber threats and attacks the Centre may need be prepared or to which they are already being exposed to.

ISSN No:-2456-2165

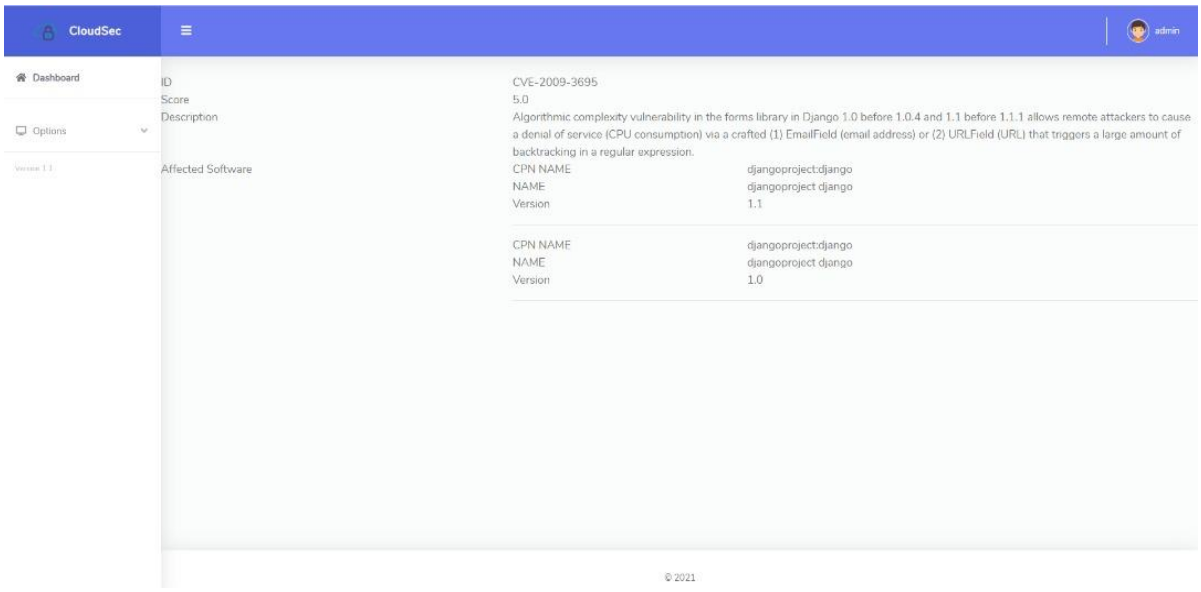

Fig. 3: Some of the detected threats to the Data Centre

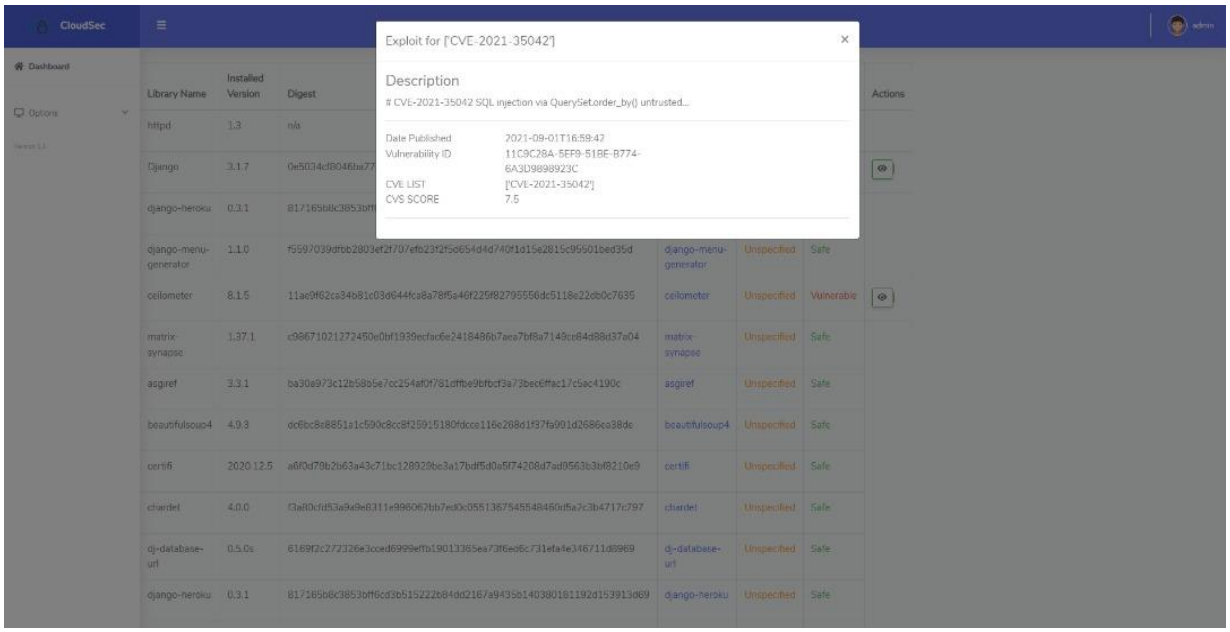

Fig. 4: Detected SQL Injection

Examination of Figure 4.1 and Figure 4.2 show that the system is not only able to detect some security vulnerabilities but also detect some threats. In the sample output from the system, the system was able to detect some possible attacks at the Centre mainly in form of denial of service (DoS). Further analysis resulted in the following list of threats being identified:

- Denial of service
- Presence of malicious codes
- SQL injection
- Spoofing, and
- DDoS

While the list was not exhaustive as the scanning for vulnerabilities was only sampled and not a complete treatment of the entire software and application suit being used at the Centre.

B. Some security vulnerabilities of the Data Centre

The hybrid data centre makes use of multiple suits of software and applications. Understanding the vulnerabilities of each suit has been the focus of several studies. However, there has been little effort put to bring together the individual vulnerabilities into a total risk score for the whole data centre. This study therefore sought to find the individual weaknesses at the facility before developing a module to calculate and define the overall risk score grade for the Centre.

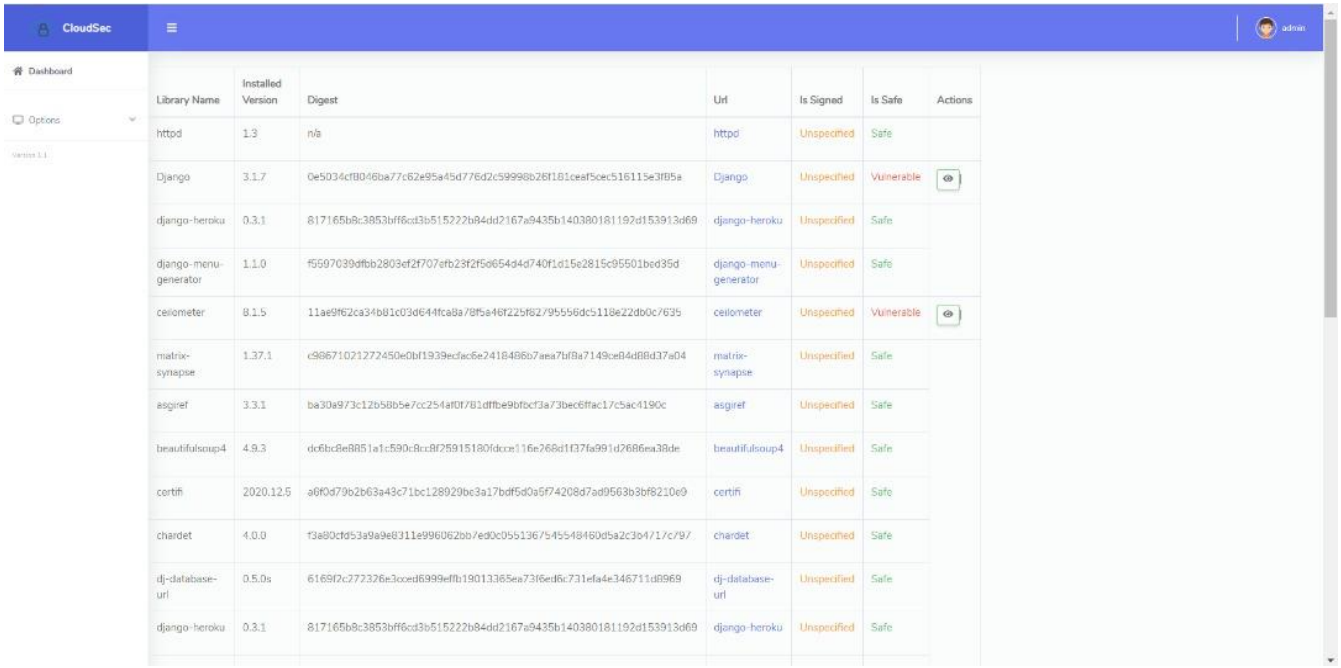

Fig. 5: List of possible vulnerabilities

The type of vulnerabilities was identified as unsafe in the system and the system would also provide the source of such vulnerabilities. Analysing the sampled vulnerabilities above, Django and Ceilometer presented the most significant vulnerabilities to the Centre. The nature of the vulnerability was coded to help standardise the vulnerabilities against known global vulnerabilities in software and applications. Each vulnerability has a unique vulnerability identify (ID) as indicated in Figure 4.2.

C. Aggregated risk score for the Data Centre

Most studies focus on identifying risk of exposure to cyber security threats for standalone systems and applications without providing some greater and holistic view of the risk level for the entire organisation based on those individual vulnerabilities. In this study, a module was created to amalgamate the individual risks for the applications and software into a unitary risk score. The unitary risk score provided some better picture of the level of exposure of the Centre to cyber security threats depending on the vulnerabilities detected.

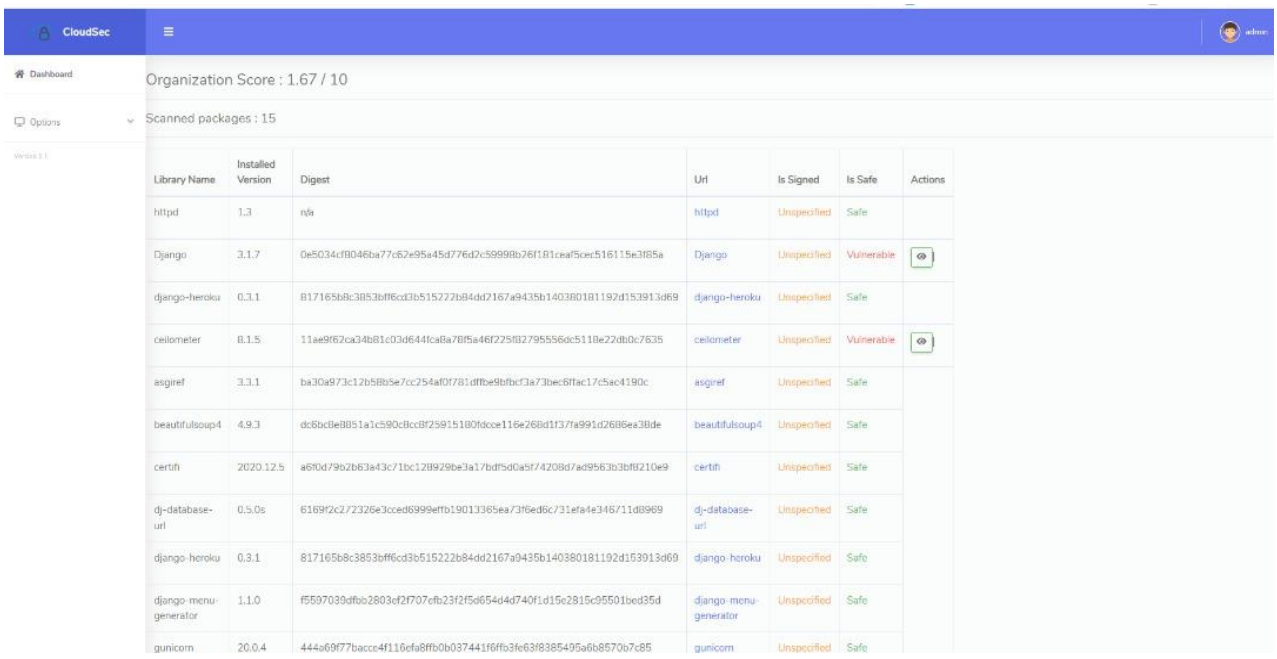

Fig. 6: Data centre aggregate organisation risk score

The module for aggregating the individual risk scores provided a sample of the aggregate risk score from the requirement file used as discussed in the Figure 3.5. Figure 4.4 shows that given the numerous vulnerabilities noted in software such as Django and ceilometer, the overall aggregated risk score was 1.67 out of a possible of 10. The given overall risk score was only for the sampled 15 software packages. The results show low level of overall risk score for the Centre.

D. Control measures to address the identified security threats at ZCHPC

The system does not only provide list of vulnerabilities, risk scores and threats detected, it also provides some interventions that may be instituted against such security weaknesses. Based on the sampled weaknesses: vulnerabilities, threats and the overall risk score, the following list of measures were proposed:

- The Data Centre to download and install patches
- Upgrade the software and application versions being used to the latest versions
- ZCHPC to decommission use of outdated software and those that are no-longer being supported
- Widen the range of software and applications being subjected to scanning and analysis of vulnerabilities using the proposed system. This is likely to give the Centre a better overview of the threats it may be exposed to.

IV. DISCUSSION

The findings of the study suggest that while it may be important to design and develop a cyber-security risk assessment framework, there are some limitations to that especially in terms of the scope to be covered and how to combine security vulnerabilities arising from computing and non-computing environment. In a hybrid data centre there are other protective security dimensions which may include personal security, physical security and document security which can hardly be captured using the methodology proposed in this study. Singh[16] summarises this dilemma by claiming that numerous risk management frameworks such as Octave, NIST and TARA have been developed from different perspectives to solve different problems. It should be expected that more such frameworks are likely to emerge under such circumstances hence the rationale for the design and development of the current risk assessment framework [14] [16]. The scope of each framework is no like the other providing each with its uniqueness. There is therefore limited chance that some findings obtained in this study may resemble some obtained from a different framework – developed under different perspectives and problem contexts.

Furthermore, risk assessment may involve some qualitative methods in conjunction with quantitative methods. However, the extent of mixing the two in a purely technical computing environment where precision can more accurately be defined using computing power may be highly unlikely. Findings from this study attests to this fact. The calculation of the individual risk score for each application and software scanned was done using a logical formula [16]. Even so the aggregate risk score was calculated as weighted sum of the individual risk scores. By doing so the risk score methodology was methodical and mathematical marginalising the corporation of qualitative risks scores. According to Granneman[10], risk management framework might need capture all security related information whether qualitative or quantitative, this claim by Granneman demonstrates that the present risk management framework is not comprehensive to stand as the mere metrics for the risk assessment management of a data centre. However, the information it contains has significant pointers to the degree of vulnerabilities of the Centre.

The results from this study provides some foundational information on the level of risk that may be found at such infrastructure though it still needs some significant improvements to be more reflective of real-life events at such critical infrastructure.

V. CONCLUSION AND RECOMMENDATIONS

The proposed risk assessment framework is no like any of the surveyed past such frameworks but helps to complement such. It adds to the perspective of managing risks at hybrid data centres. Ability to capture the human perspectives through creation of comprehensive requirement.text files helps to capture not only the technical details of the threats but also considers the human perspectives enriching the way risk is calculated and defined.

Hybrid data centres have no unique vulnerabilities and threats than other computing infrastructure. However, it seems some vulnerabilities and threats are more common for the data centres than other infrastructure. In this study, denial of service and malware are some of the threats which are peculiar to data centres. Furthermore, due to complexity in the mixture and combination of software and application suit at a data centre, the range of threats may not be predefined nor generalised from one centre to the other. Empirical testing and verification of these weaknesses need customised and personalised approach as indicated in this study.

- Recommendations

Given the divergence and uniqueness of the proposed framework with previous frameworks, the following can be recommended:

- For a comprehensive risk assessment framework that does not capture computing-related threats and vulnerabilities, further research is pertinent that also captures the human perspectives and other security dimensions such as the physical and personal security issues at the data centre. Better future frameworks may need to incorporate not only the quantitative risk assessments but incorporate the qualitative elements to risk.
- Designing and development of a comprehensive risk assessment framework for a complex working environment such as a data centre requires more time than may be that afforded in this study. This may provide the opportunity to identify all applications, software and

other assets of the Centre whose well-being requires proper risk management systems to be instituted.

REFERENCES

[1.] Mtetwa, "Exploring cyber security threats in Zimbabwe," Parliament of Zimbabwe , Harare, 2017.
[2.] Harare Institute of Technology, "IT students tour Zimbabwe Centre for High Performance COmputing (ZCHPC)," Harare Institute of Technology (HIT), Harare, 2020.
[3.] C. Cimpanu, "Supercomputers hacked across Europe to mine cryptocurrency," University of Stutthart, Germany, 2020.
[4.] M. Huey, "US leadership in HPC: A report from the NSA-DOE technical meeting on high peerformance computing," NSA-DOE, New York, 2016.
[5.] McGovern, "Supercomputers can spot cyber threats," Techplore, USA, 2019.
[6.] D. Bufnea, V. Niculescu, G. Silachi and A. Sterca, "Babes-Boyai University's High Performance Computing Center," *Informatica*, vol. 61, no. 2, 2016.
[7.] R. Brandt, "Supercomputing challenges and predictions," Institute of Electronic and Electrical Engineers (IEEE), Washington DC, 2013.
[8.] C. Servin, "Challenges of securing a Petascale Cluster," The University of Texas, El Paso, 2011.
[9.] S. Peisert, "Cybersecurity for HPC Systems: State of the art and looking to the future," University of California, California, 2018.
[10.] J. Granneman, "Top 7 IT security frameworks and standards explained," Fotolia, USA, 2020.
[11.] N. Alshareef, "A model for an information security risk management (ISRM) framework for Saudi Arabian Organisations," in *International Conference ITS*, Saudi Arabia, 2016.