The Seybold Report

ISSN 1533-9211

IDENTIFY AND CLASSIFY CRITICAL SECURITY ISSUES FOR BIG DATA BASED ON CLOUD COMPUTING IN HEALTHCARE ORGANIZATIONS

MONTASER B A HAMMOUDA , ARIFF BIN IDRIS, MOHAMED DOHEIR

Fakulti teknologi maklumat dan komunikasi(FTMK),
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

DOI: 10.5281/zenodo.6553720

Abstract

Cloud computing is becoming increasingly popular in the distributed computing environment every day. Cloud environments are used for data storage and processing. In addition, Big Data based on cloud computing is a new technology in Palestine and generally in the Arab states, research and articles executed mostly for foreign states. Big data implemented and succeed in health organizations and hospitals, but there are several issues faced implementation of Big Data especially in security and privacy, cultural and organizational challenges especially because of political situation in Gaza Strip. The aim of this study is to identify and classify security issues for big data based on cloud computing in healthcare organizations. Further, modelling security issues for big data based on cloud computing in healthcare organizations. The result shows that 25 critical security issues for big data based on cloud computing and classified it to four groups based on architectural, operational, technological, organizational security challenges face the implementation of cloud computing environment for big data. A successful identify security issues for big data based on cloud computing will greatly improve the probability of applied cloud computing in healthcare organizations. In the area of big data based on cloud computing, there is still a clear gap that requires more effort from the research to build in-depth understanding of performance characteristics of big data based on cloud computing. We consider this study a step towards enlarging our knowledge to understand the big data based on cloud computing and provide an effort towards the direction of improving the state of the healthcare and achieving vision on the big data-based cloud computing domain.

Keywords— Big Data**,** Cloud Computing**,** Healthcare Organizations**,** Security Issue

1 Introduction

As a result of the rapid growth of new applications such as analysis of bioinformatics network, social network, and semantic Web, several type of data to be processed continues to rise every day. An interesting but critical challenge is the effective management and analysis of broad-based data. Big Data from academia, industry and government has recently attracted a lot of attention (Sakharkar, Dande and Mate, 2017). Cloud computing is becoming increasingly popular in the distributed computing environment every day. Cloud environments are used for data storage and processing. Cloud computing provides internet-based applications, platforms and infrastructure. Cloud computing is a model for enabling convenient network access, on demand and with minimal management effort or service provider interaction, to a shared pool of configurable computing resources (e.g. networks, server, storage, applications and service) (S and Guruprasad, 2015). Big data contains a large amount of data which can be processed to output value from raw or analysed data based in architecture and new technologies (Sakharkar, Dande and Mate, 2017), its characteristics classified in three dimensions shortened in 3V: Variety in the type of data, volume of data and velocity in processing (Suthaharan, 2014), while (Gandomi & Haider, 2015) shortened it in size of data

The Seybold Report
ISSN 1533-9211

and at times. Big data based cloud computing technologies introduce effective interventions and reduce cost in organizations(Fun, Samsudin, & Zaaba, 2017) and affect human resource hierarchy in firms, procedure in decisions making. it is considered not only technological change in healthcare organization, delivery ways of outputs, and technological infrastructure but it needs another change to take place such as culture of the organization and users outside the organization, execution of new work models, environmental dimensions, and how to implement this application securely and who to keep privacy of new system. Big Data in cloud means huge and historical data kept for long time, low errors, high accuracy, new ways of monitoring, evaluation and tracking errors, reports preparing by one click, diseases predicting. Patients are main element of the process in big data and in upgraded stage they not only have access to show their documents, dosages, therapies, but they can feed data through their machines such as mobiles, PCs, sensor machines. In cloud, parallel computing processes implemented in the same time, complex data stored in several nodes and linked together to work in one system. File system called HDFS used to enhance reliability in storing and recalling files from several nodes to avoid failure in nodes and data lose (Saraladevi, Pazhaniraja, Paul, Basha, & Dhavachelvan, 2015; Securosis, 2012).

Many institutions and organizations use cloud computing to competitively improve their business with the same or lower cost. But the reticence with adoption is related to safety performance; many still expect a model that will enable them to rely on powerful, secure public clouds to store and access their private data (Singh, 2017). Cloud computing technologies are used to rent resources under three models: IaaS, PaaS, and SaaS. Cloud computing is used to rent resources under three models. In addition, we can use a cloud-based terminal, connect cloud-based software services to your browser or client, also order related service software to meet their needs, and pay a fee. SaaS is a cloud server software application for service providers. As long as the web terminal is present, the user will be allowed to take advantage of cloud services; the vendor will manage the upgrade of cloud server hardware and software maintenance (Hao, 2016). The cloud is also available upon request. The applications available via web browsers are intended for end-users in this service model (Mahalakshmi, 2017). In addition, we have distinguished ourselves in the SaaS layer as software providers and service providers. The software providers are focused on digital content and applications. Post-sale and value-added service support for service providers (Wu and Chang, 2013). The main goal of this study is to propose modelling security issues for big data on based cloud computing in healthcare organizations in Gaza. The aim of the study is to identify and to classify security issues for big data on based cloud computing in healthcare organizations.

1. Research Methodology

Managing security issues in big data requires adopting cloud computing technology. However, we will propose model for managing critical security issues for big data based on cloud computing in healthcare organizations. Further, the new big data based on cloud computing model will be developed to classify and create relation between critical security issues factor. Managing critical security issues for big data based on cloud computing in healthcare organizations are crucial. Therefore, this study proposes new model for predict critical security issues for big data-based cloud computing. The model will be validated by

The Seybold Report
ISSN 1533-9211

using quantitative techniques. Furthermore, the security issues are identified in all the phases of the cloud computing for big data based on the literature.

2. Cloud Computing

Cloud computing technology is a significant topic in organizations of academic and business. The business process is developed and implemented in distributed, freely linked environments and in combined services, including more services, and therefore a diverse design and approach connects the cloud of services. There are many functionally similar cloud services available, as they include on-demand service, quality of cloud service factors and SLAs needs (Sasikaladevi, 2016).

3. Challenges in implementing of Big Data based cloud computing projects

In the IT industry, cloud computing has created a remarkable paradigm shift and brought several benefits such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These advantages made it possible for cloud to have a significant impact on various smart cites sectors. Cloud adoption has, however, increased the sophistication of the ever-changing security risks that frustrate companies when they expand their on-site infrastructure to cloud horizons (Damenu and Balakrishna, 2015). Several studies in the area of big data projects refer to the challenges and obstacles to its successful implementation. In slow health, culture and organization, it is particularly important (McAfee, Brynjolfsson, Davenport, Patil, & Barton, 2012), besides a shortage of skilled lab (Chen, Chiang, & Storey, 2012) Barriers to supporting top management are also considered. Cloud delivery models offer exceptional flexibility, allowing IT to assess the best approach to the request of each business user. For example, organizations that already support an in-house private cloud environment can add Big Data Analytics to their in-house offerings, use a cloud service provider, or build a hybrid cloud that protects some sensitive data in a private cloud but uses valuable external data sources and applications in public clouds (Sakharkar, Dande and Mate, 2017). In addition, privacy and security of data are a major obsession for companies. (Feldman et al., 2012). And the future added value generates the high costs of Big Data investments stand-up, in conjunction with a lack of vision difficulty. It is therefore essential that an organization or community is "ready" to implement big data projects before making a costly investment. Through this, sound research must take precedence over the introduction of Big Data into healthcare in Gaza and highlight barriers and facilitators that can guide successful Big Data Ma planning and implementation when addressed by policy makers. In Study: The research is based on a Gaza Public Hospital that provides caution to Palestinian healthcare's widespread outcomes and seeks to identify key barriers and opportunities to implement Big Data projects in Palestinian hospitals in the Strip (Elsirr, 2018). According to (Atallah, 2017), studies on the impact of the e-Health Information System (HIS) UNRWA-Gaza's primary healthcare centres, 286 questionnaires from the total population collected from 22 centres, showing a positive connection to the e-Health Information System and the quality of care. Relative advantages and compatibility during its usefulness have a direct effect on medical error prevention and reduction. Perceived usability and relative benefits are increasingly having a significant influence on health care improvements. In addition, relative benefits and compatibility have a direct impact on the redesign of patient care. The designer of the system

The Seybold Report
ISSN 1533-9211

should explain and facilitate the indication of alerts and error messages problem solutions. Patients should also have access to their medical records of their own. Starting a patient portal website is therefore essential. And it should also be improved in order to support X-ray physiotherapy. Cloud Computing Security is therefore a new emerging computer security area that refers to the set -of primitive policies, controls and encryption to protect online data, system applications and infrastructure (Raja & Hanifa, 2017).

4. Cloud Service Models

Cloud computing is a service that provides CSP customers with facilities and self-service. There are three types of cloud services: as a service software (SaaS), as a service platform (PaaS) and as a service infrastructure (IaaS) (Isaac et al. 2018). The prevailing evolution of distributed, parallel and grid computing is accelerated development in cloud computing. The result of this cloud computing is Cloud, Cloud Virtualization, IaaS, SaaS, PaaS conceptual mixing devices (Fu, 2016).

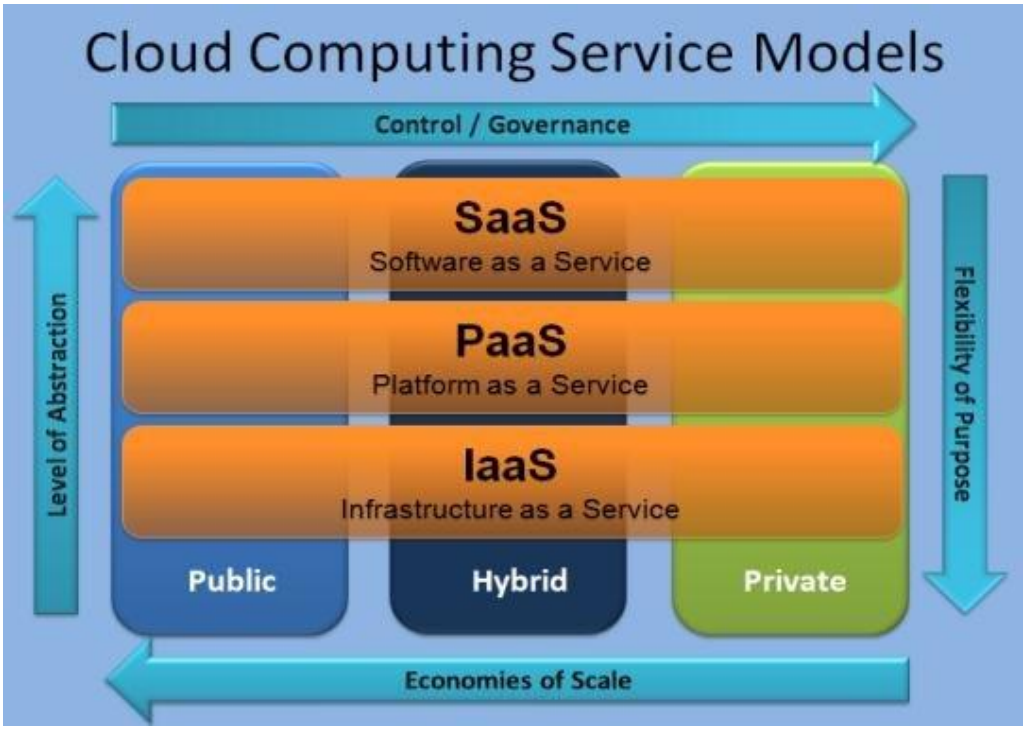

Figure 4.1 Service Models for Cloud (ResearchGate, 2019)

The Seybold Report
ISSN 1533-9211

5. Cloud Deployment Models

The cloud deployment model involves public cloud, private cloud, and hybrid cloud as can be seen in the Figure 2.2.

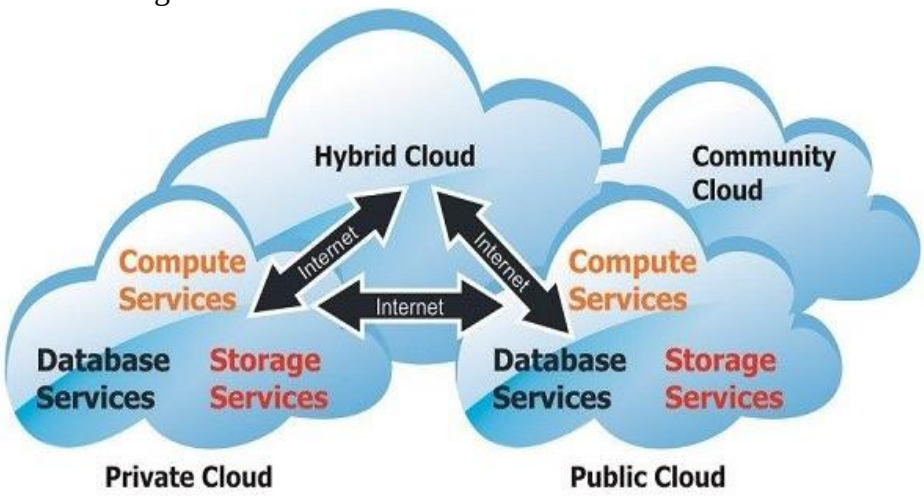

Figure 5.1 Cloud Deployment Models (BesantTechnologies, 2018)

6. Critical Factors Leading to security issues in big data-based Cloud Computing System

Remarkably, the most important factors in the event of failure or success were those of these studies: project integration management, scheduling, integrated project management, performance assessment, project performance information, business environment factors, process assets ; technology and toll management, technical complicity and novelty, and human resources project management are success criteria acting as spring board toward project prosperity (Taherdoost & Keshavarzsaleh 2015). Because of technical differences between major service suppliers, compatibility issues arise in an appropriate format based on the VM of several cloud systems (Weixiang & Lin 2016). It is a major outcome of the organization's development strategies. The attendance of supporting cloud computing functions, such as statistical analysis, may contribute to the creation of effective compensation plans for multinational companies operating around the world. The system can easily organize custom compensation plans on the cloud platform and react to them immediately with other existing compensation policies. However, in advanced technologies such as cloud computing that are vulnerable to cyber gaps that adversely affect the safety and privacy of electronic health records of patients, and in these situations, the wireless networks ' security challenges need to be carefully understood and considered. Recently, security concerns in the cloud computing environment are increasingly challenging (Mehraeen, Ayatollahi, & Ahmadi, 2016). The recent

The Seybold Report
ISSN 1533-9211

rise in block chain technologies has enabled organizations to leverage a secure distributed public ledger where important information could be stored for different purposes, including greater transparency of underlying economic transactions (Kantarcioglu, 2019).

6.1 Architectural Issues

6.1.1 Distributed Nodes

The way to Big data is "Data Moving is expensive than computing moving", processing can be implemented anywhere because of availability of resources, but these concept introduce new environment which can be not homogeneous and distributed processing platform, and probability of hacking and cracking the system will increase (Securosis, 2012), so it is not easy to make security verification about the place of computing (Inukollu, Arsi, & Ravuri, 2014).

6.1.2 Shared data

Data in cloud move with numerous copies shifting to and from distinct machines to guarantee redundancy and resilience. Shard is a data segment take part through several servers, auto-motion of Shard in several nodes makes it hardly to determine the location and the number of copies. Protection of data in traditional way in centric server/s cannot be used in cloud, where big data stored and move according to users' request from location to another. "The data security model ' containerized ' is missing, as are many other facilities for relational databases"(Securosis, 2012).

6.1.3 Internode Communication

With the use of RPC over TCP / IP, there is a lack of security in Hadoop communication and most of the distribution. In big data distribution, SSL and TLS are scarcely packaged. If they address communication from client to proxy, as with HDFS proxy servers, they do not communicate from proxy to node, Remote Procedure Calls (RPC) must fall over SSL (Securosis, 2012) (Inukollu et al., 2014).

6.1.4 Data access/ownership

Access of users to reach data is essential concept in security of database. Generally, environments of big data introduce limitations for users' access in several levels of access, but this is in less accuracy of access. The security of labels, groups, roles, and other issues in big data environments can be implemented rationally, but this needs designer to construct features into apps and data storage(Securosis, 2012). Access control scheme is a safe technique in cloud computing infrastructures to trust data security. With the polynomial interpolation of Lagrange to establish a secure and effective access to health care information scheme, it enables accurate access to control and is suitable for huge multi-users. Although the identity of the user, the mechanism for multi-biometric encryption and data auditing to verify the accuracy of health care data are other ways to ensure the security of information stored in the cloud. At the entry of all accesses, the identity of the user should be verified using the username and password assigned by the cloud providers. Authorization is a critical security requirement for controlling cloud ownership of access priorities, permissions, and user sources. Cloud users have the right to access information on their account.

The Seybold Report
ISSN 1533-9211

6.1.5 Client interaction

Sometimes, interaction occurs in system's users where client gain rights of managers and reach nodes and resources of data; malicious can use these rights to make bad actions inside the system. In this model, it communicates efficiently but it is hard to prevent client to reach nodes. Worse still, the distribution of self-organizing nodes is a bad fit for security tools like gateways and firewalls and bad in tracking and auditing that require a ' choke-point ' that is not available in mesh cluster (Securosis, 2012). However, we use customer interactions to provide IaaS-level self-management websites that effectively shoulder some of the cloud service providers ' network load. Building black and white lists gradually reduces the number of potential IPs and IT security events (Yang & Cheng, 2015). Connecting all kinds of equipment and assets by sensors, however, and maintaining real-time monitoring of key equipment status allowing interaction and instant connection between multiple users. By adapting powerful computing capacity from cloud computing, we can implement integrated information analysis, perform real-time, high-speed and two-way transmission, and achieve the goal of greater grid reliability and availability (Yang, 2012).

6.1.6 No-Security

This concept relies on lack of security when we use cloud generally, several attacks for data storage can be occurred through authorization-based role-access, web proxy, no facilities can make system fully secured to protect apps, data storage, and most big data APIs are susceptible to known assaults. Health care organizations should have direct control over many aspects of security in order to ensure data security in cloud computing infrastructures. Health care providers are generally very confident in cloud service providers in this area. Cloud service providers play a key role in the response to incidents, including transaction analysis, access control, data protection, rehabilitation and integration of services (Mehraeen et al., 2016).

6.2 Operational Issues:

In operating cloud systems, infrastructure as architecture security issues are important, but we have to protect applications from attackers in order to keep data secure from stealing or any sabotage actions, Shortlisted of 12 top security violation in cloud listed by (CSA, 2016): Data violation, Compromised certificates and cracked authentication, Hacked interface and application program interfaces, exploited system vulnerabilities, account hacking, malicious insiders, parasite Advanced Persistent Threat(APT), permanent data loss, inadequate diligence, abuse of cloud services, Denial of Service(DoS) attacks, shared technology, shared hazards (Subramanian & Jeyaraj, 2018).

6.2.1 Distributed Data

Securities confirmed that excessive data which distributed in several nodes or machines is an essential characteristic of Big Data. But according to the environment of cloud, it is highly hard to discover precisely where parts of a file are stored. but these parts of data were stored in node or machine depending on availability and repair activities, in conventional system all data in main store and protected with several tools of security, but this concept is not compatible with cloud environment (Inukollu et al., 2014; Securosis, 2012). In fact, cloud networking considers the network beyond data centres in order to provide on-demand computing as well

The Seybold Report
ISSN 1533-9211

as network resources. Cloud networking can provide resources and services through the interconnection of distributed data centres owned by one or more cloud data centre networking providers (Luong, Wang, Niyato, Wen, & Han, 2017). Key technologies such as data mining searches, etc. Using virtualization, mass distributed data storage, distributed mobile cloud computing overcomes MCC's performance-related data management, parallel programming model, wireless barriers such as bandwidth, storage capacity and battery life, networks and security, etc. in order to deliver MCC's implementation goals as well as environmental issues such as availability (Yadav, 2016).

6.2.2 Protection of Data

Several environments of cloud such as Hadoop have no coding for their data, they only keep it without any changes, but this is considered as a risk because of accessing probability of hackers and they can mooch vital or critical data from machines (Inukollu et al., 2014; Securosis, 2012). To ensure confidentiality, integrity and availability, the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction (Rogers, 2016). The architecture study security issues of cloud computing from data storage and data security aspects are proposed based on Cache data storage model based on third party certification and data security mode, thus improving data availability, data transfer from storage, establishing appropriate protective measures to achieve effective protection of cloud data (Yang, 2016).

6.2.3 Data at rest protection

Encryption introduce constraint of data entry to prevent clients to inter any data not compatible with the interface of the apps in nodes/machine. Encrypted data protected from users (clients and managers) whom can reach servers and make softcopy where the data is valueless without owning keys of encryption. It is a critical problem that usually encrypted data lacks adequate scalability and transparency to operate with big data environment (Securosis, 2012), Hash file and cloud meta-data enhance the security of cloud data stored, while (Chatterjee, Roy, & Scholar, 2017) introduced methods for check data security in the cloud, in usage of cryptographic settings to keep privacy. Additionally, data security issues for cloud storage system in the application process facing, this paper presents secure data storage architecture based on cloud computing (Yang, 2016).

6.2.4 Administrative Rights for Nodes

All data are available for administrative and they can reach to critical date of users without control (Inukollu et al., 2014), so we have to know if the system record actions that administrator do, there is a limited access of them to some data or not, and if there is a limited access to quantities of data can be copied from administrators. There are two applications one is to provide the administrative rights used by the administrator whereas second is used by the employees in order to notify the work assigned to them has been done. The functions performed by the administrator are assignment of the job and location and view the location details of the employee. The functions which the employee performs are face recognition and sending the notification whether the job assign has been completed or not (Basu et al., 2016).

The Seybold Report
ISSN 1533-9211

6.2.5 Authentication of Applications and Nodes

Nodes may participate clusters to boost practices at the same time. In the event of no Authentication, third-party nodes/machines may participate clusters to rob information /data or interrupt cluster practices (Inukollu et al., 2014). And enable verification for users, machines/nodes and apps (Archenaa & Anita, 2015). Developing Authentication for the Cloud Computing. "I know, I think" so I refuse or accept the change in procedures or new systems of the organization, this is the main challenge of employees or managers' culture (Dutta & Rose, 2015). Data are important for getting value for organization and introduce high accuracy in making data-driven decisions, not only relying in experience of employees or managers (McAfee et al., 2012). Routine in health organization is a challenge to obtain adoption of Big Data (Ilahi, Ghannouchi, & Martinho, 2014). It is fundamental in hospitals to make changes at the structural and organizational level and it is important to study existing work systems (Manenti, Goyet, Reinicke, Macdonald, & Donald, 2016). The process of validating and ensuring the identity of cloud service subscribers or users is authentication in the cloud context.

6.2.6 Logging and audit

Lack of Logging in cloud lead to absence of tracking several actions such as data deleting and modifying, and to determine the identity of hackers who access, make actions, breached clusters, or did any bad or dangerous behaviour (Inukollu et al., 2014) (Archenaa & Anita, 2015). Logging is a tool that provides a range of pass-on functionality, Scribe and Logstash are classified as tools for open source in several Big Data settings, we have to choose suitable tool, and use it and make integration with systems like log management or SIEM, and finally outputs evaluation. Data reviewing and policies to discover frauds are important to get beneficial logging (Securosis, 2012). Like many application domains, cyber security is gathering more and more data. Examples of these data are system logs, traces of network packets, account login, etc. As the amount of data collected is increasing, it has become impossible to manually analyse all the data collected to detect and prevent attacks (Kantarcioglu, 2019)..

6.2.7 Administrative data access

Every machine/node has its own (client) who has full access to all data in his node, but there are several limitations of validity for managers to reach clients' data, this problem solved by combining of two ways, the first is access controls, and the second is encryption technologies which contribute in making protection to reach or exploit clients' data (Securosis, 2012).

6.2.8 Monitoring, filtering, and blocking

There is no tool that can monitor and block attackers, and there is no unanimity on security attack query, while Kerberos can be used to authenticate users while "MapReduce access is gated by digest authentication. Several monitoring tools are available for large data environments, but most of the API layer review data and user requests"(Securosis, 2012). Authorization Management Program (' FedRAMP ') applies a standardized approach to monitoring the security of cloud computing services and products and allows providers to qualify for cloud computing services in federal procurement (Dimitri and Apostol, 2016). In

The Seybold Report
ISSN 1533-9211

fact, by monitoring data access, the cloud server could exploit the frequency information with which different pieces of information are accessed to reconstruct the correspondence between the plaintext data and the encrypted data (Sabrina, FOresti and Samarati, 2012).

6.3 Technological issue

Because of technical differences between major service suppliers, compatibility issues arise in an appropriate format based on the VM of several cloud systems (Weixiang & Lin 2016).

- **Security risks for cloud computing and network**
- **Encryption in Cloud Computing**
- **Storage Security at the CSPs Data**
- **Biometric Security System for Healthcare Big Data Based Cloud Computing**
- **Traditional Security System Tools**

6.4 Organizational Dimension

It is a major outcome of the organization's development strategies. The attendance of supporting cloud computing functions, such as statistical analysis, may contribute to the creation of effective compensation plans for multinational companies operating around the world. The system can easily organize custom compensation plans on the cloud platform and react to them immediately with other existing compensation policies.

6.4.1 Confidentiality in Big Data based Cloud Computing

Data confidentiality is at the top of this technology's list of security concerns. Many methods have been introduced to overcome this problem; encryption is one of these methods and widely used to ensure data confidentiality in the cloud environment (Soofi and Khan, 2014). Data security goals include three confidentialities, availability, and integrity points. Cryptography can achieve confidentiality of data in the cloud (Soofi and Khan, 2014).

6.4.2 Access control

Meanwhile, access control is more concerned with making it possible for a user to access several cloud resources. While this process is typically handled by accessing applications, consideration is now being given to centralizing the decision on the authorization policy regardless of the user's location or application. Implementing proper access control models for the cloud is one of the areas that has been critically assessed since current access control models are not specifically designed to address cloud systems requirements (Lim et al., 2017). Providing authentication, authorization and access control within the virtualized network of the cloud is important..

The Seybold Report
ISSN 1533-9211

6.4.3 Use of Different Technologies

Cloud environment contains of several technologies and components such as network, database, operating systems (Windows, Lunix, Android, IOs and another systems) (Khrisna & Harlili 2014) and stuff; In this environment, any small breakthrough in security may put all the system in danger, this diversity need security maintenance and it classified highly important in challenges faced security(Inukollu et al., 2014). Localization work, however, primarily falls into either technique based on infrastructure or peer-based techniques. Methods based on infrastructure use technologies such as GSM, Wi-Fi, RF, GPS, RFID, and IR ultra-sound. Current GPS works very rarely indoors, and the more accurate techniques require additional infrastructure and dense deployment of access points (Fernando, Loke, & Rahayu, 2013).

6.4.4 Abuse and Nefarious Use of Cloud

Since cloud computing offers various on-demand computing services in low cost and sometimes free trial versions, people can misuse these services to their advantages (Bamiah, Brohi and Chuprat, 2012). By misuse of relative anonymity behind cloud registration and models of use, malicious activities can be carried out with relative impunity (Cayirci, 2013).

6.4.5 Security and Privacy Issues in Big Data based Cloud Computing

Several security and privacy issues face the implementation of Big Data based cloud computing, which must be considered to protect data from hackers and crackers. Cloud computing has many security problems because it includes various technologies in networks, databases, resources timetable plan, transaction managing, loading issues, virtualization ,parallel processed control and managing of memory, operating systems (Inukollu et al., 2014). Privacy is a person's desire to control personal information about the user. In the cloud, many possibilities can damage cloud user privacy, such as insider user threats, external attacker threats, data leakage, etc. (Yadav and Doke, 2016). Users need to know exactly what personal information is visible to the public and control their personal data stored on their smartphones. It is essential that any personal data shared is done with the consent of the user and that at any time they can opt out of any data collection program (Fernando, Loke and Rahayu, 2013). Although a major issue, little research has been done in this regard. Existing cryptographic techniques can be used to secure data, but protection of privacy and outsourced computing require considerable attention. Personal data should always remain in the control of the user and the user decides with whom and with whom they share their data. Especially when cloud authentication strategy is used implicitly and context-conscious, the identity provider needs access to real-time user information (Lim et al., 2017). The security tree in Fig 3.4 shows the significance of fundamental safety requirements (Subramanian & Jeyaraj, 2018), we mentioned some issue below:

The Seybold Report
ISSN 1533-9211

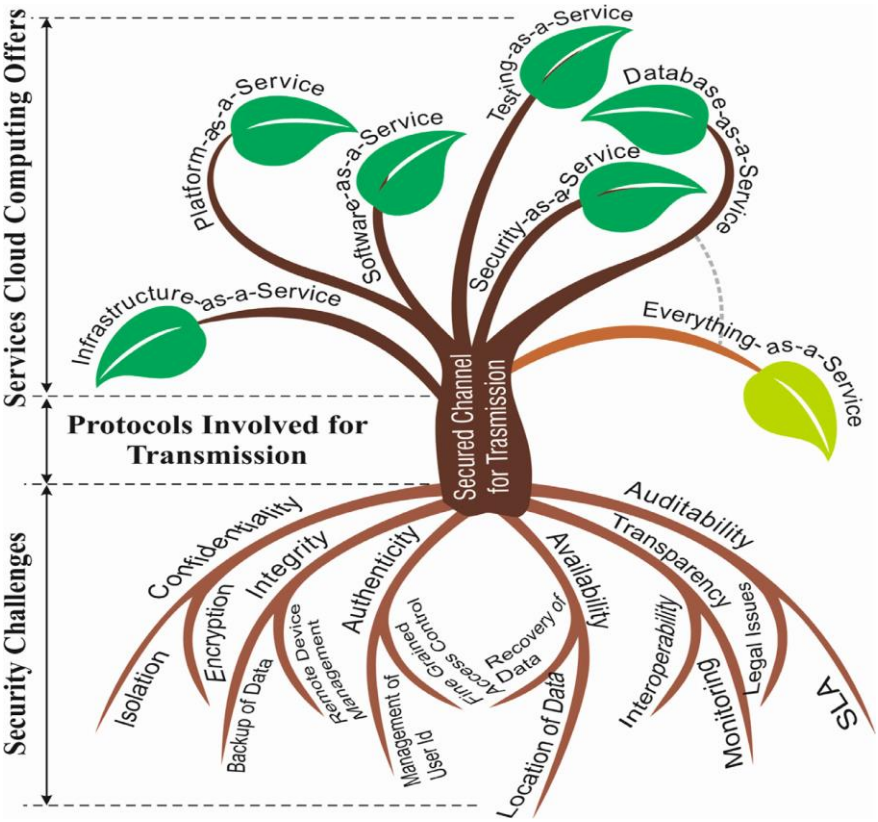

Figure 6.1 The Security Tree(Subramanian & Jeyaraj, 2018)

6.5 Trust

Cloud service providers and users agree with the signing of a trust agreement, agreement on security issues upload, download, edit, and management of data, and thus the cloud data management platform to achieve oversight mechanisms, and to constrain the behaviour of cloud service providers. Even signed a corresponding agreement, whether the cloud service providers to comply with certain legal constraints policies and agreements, and related policy and legal constraints cloud service providers in efforts to what extent, these are the users need to consider Security risks for network (Yang, 2016). Trust plays an important role in the selection of services. It is a tedious task to select the trustworthy service with the cost and other constraints for service composition. This paper proposes a method for estimating service trust based on the distribution of Beta (Sasikaladevi, 2016). A trust management system that enables mobile users to use cloud computing by trusted mobile cloud providers(Hussain and Almourad, 2015). However, in order to support customers in reliably identifying cloud service providers, this work offers a selection of cloud service providers (SCSP) framework that includes trustworthiness, interaction risk estimation skills, data backup and data recovery. Trust worthiness is gained from feedback on service providers ' reputations (Patil, Patil and Patil, 2017). Thus, trust-aware service brokering scheme to effectively match cloud services (or resources) to meet various user requests.

The Seybold Report
ISSN 1533-9211

7. The model: Adaption of security issues for big data in cloud computing for healthcare

In this model, we will determine the critical security issues for big data in cloud computing for healthcare organizations in all components of Big data and cloud computing.

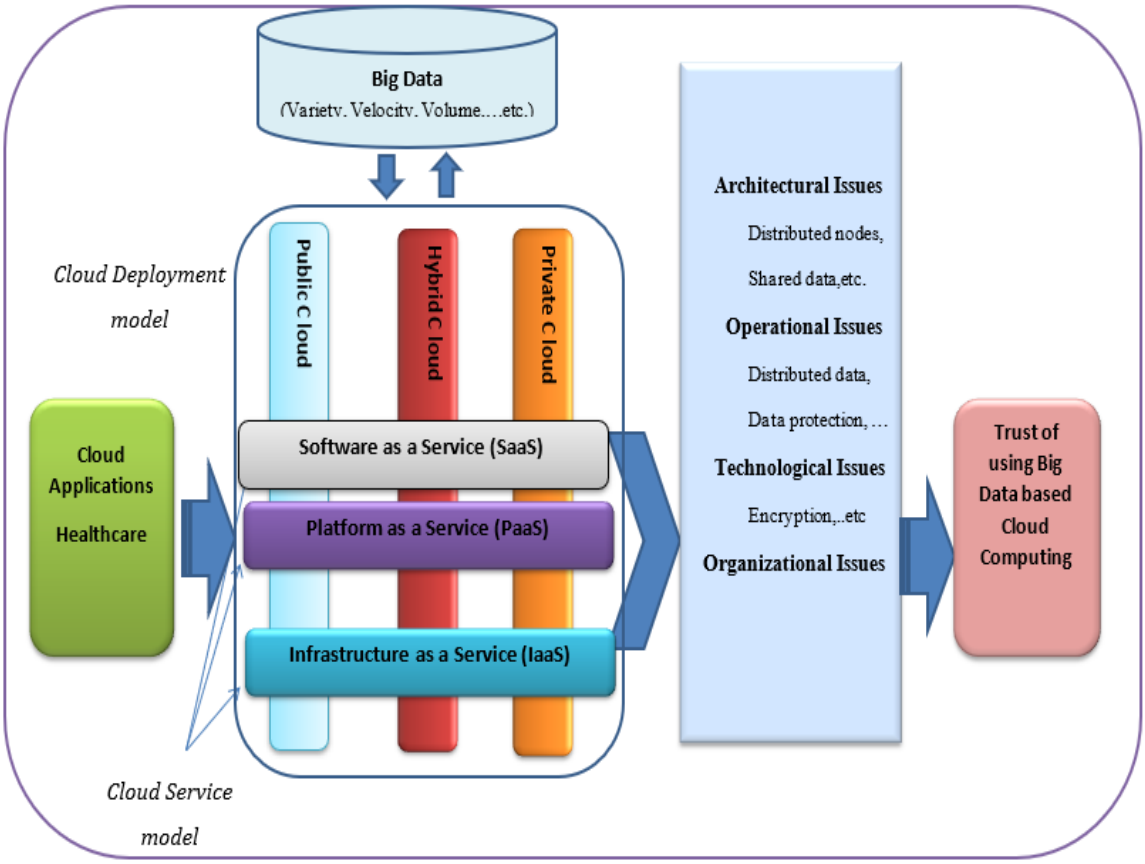

Figure 7.1 Modelling for security issues for big data in cloud computing for healthcare

8. Conclusions

We determined the critical security issues for big data on based cloud computing in healthcare organizations. The aim of the study is to identify and classify security issues for big data based on cloud computing in healthcare organizations. Further, modelling security issues for big data based on cloud computing in healthcare organizations. The result shows that 25 critical security issues for big data based on cloud computing and classified it to four groups based on architectural, operational, technological, organizational security challenges face the implementation of cloud computing environment for big data. A successful identify security issues for big data based on cloud computing will greatly improve the probability of applied cloud computing in healthcare organizations.

The Seybold Report
ISSN 1533-9211

9. REFERENCES

- Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data, 5*(1), 1.
- Ahmad, M., Pervez, Z., Lee, S., & Kang, B. H. (2015). *Task-oriented access model for secure data sharing over cloud.* Paper presented at the Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication.
- Ajami, S., & Arab-Chadegani, R. (2013). Barriers to implement electronic health records (EHRs). *Materia socio-medica, 25*(3), 213.
- Archenaa, J., & Anita, E. M. (2015). A survey of big data analytics in healthcare and government. *Procedia Computer Science, 50*, 408-413.
- Atallah, A. A. (2017). The Impact of E-Health Information System (HIS) Characteristics at UNRWA-Gaza Health Centers on Healthcare Quality. *The Impact of E-Health Information System (HIS) Characteristics at UNRWA-Gaza Health Centers on Healthcare Quality*.
- Bamiah, M., Brohi, S., Chuprat, S., & Brohi, M. N. (2012). *Cloud implementation security challenges.* Paper presented at the 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM).
- Basu, D., Indusai, G., Vijayashree, J., Jayashree, J., Caytiles, R. D., & Iyengar, N. C. S. (2016). Analysis and Issues in Cloud Operating System. *International Journal of Grid and Distributed Computing, 9*(11), 179-186.
- Bennani, A., Belalia, M., Oumlil, R. (2008). *As ahuman factor, the attitude of healthcare preatitioners is thr primary step for the e-health: First outcome of an ongoing study in Morrocco.* Paper presented at the communications of the IBIMA
- BesantTechnologies, J. t. i. C. (2018). Cloud Deployment Models. from https://bestjavacourseinchennai.wordpress.com/2018/10/06/a-course-guide-to-cloud-deployment-models-2018/
- Cayirci, E. (2013). *Modeling and simulation as a cloud service: a survey.* Paper presented at the Proceedings of the 2013 Winter Simulation Conference: Simulation: Making Decisions in a Complex World.
- Chandrashekar, R., Kala, M., & Mane, D. (2015). Integration of Big Data in Cloud computing environments for enhanced data processing capabilities. *International Journal of Engineering Research and General Science, 3*(3).
- Chatterjee, R., Roy, S., & Scholar, U. (2017). Cryptography in cloud computing: a basic approach to ensure security in cloud. *International Journal of Engineering Science, 11818*.
- Chaturvedi, A., & Lone, F. A. (2017). Analysis of Big Data Security Schemes for Detection and Prevention from Intruder Attacks in Cloud Computing. *International Journal of Computer Applications, 158*(5).

The Seybold Report
ISSN 1533-9211

- Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS quarterly*, *36*(4), 1165-1188.
- Chouhan, P., & Singh, R. (2016). Security attacks on cloud computing with possible solution. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6*(1).
- Chuang, Y.-T. (2016). CIRCLE: A cloud-based mobile wellness management system. *Journal of Biomedical Engineering and Medical Imaging*, *3*(6), 68.
- CSA, W. K. C. s. a. (2016). The treacherous 12: cloud computing top threats in 2016. from https://cloudsecurityalliance.org/articles/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/
- Dutta, D., & Rose, I. (2015). Managing a Big Data project: The case of Ramco Cements Limited.

- . *International Journal of Production Economics*.
- Elsirr, B. J. (2018). *Big Data Management In Gaza Strip Hospitals: Barriers And Facilitator.* (Master), IUG.
- Esa, D. I., & Yousif, A. (2016). Scheduling Jobs on Cloud Computing using Firefly Algorithm. International Journal of Grid and Distributed Computing, 9(7), 149-158.
- Elzamly, A., Hussin, B., Naser, S. S. A., et al. (2015) 'Predicting Software Analysis Process Risks Using Linear Stepwise Discriminant Analysis: Statistical Methods', International Journal of Advanced Information Science and Technology (IJAIST), 38(38), pp. 108–115.
- Elzamly, A. and Hussin, B. (2014c) 'Evaluation of Quantitative and Mining Techniques for Reducing Software Maintenance Risks', Applied Mathematical Sciences, 8(111), pp. 5533–5542.
- Elzamly, A., Hussin, B. and Salleh, N. (2016) 'Top Fifty Software Risk Factors and the Best Thirty Risk Management Techniques in Software Development Lifecycle for Successful Software Projects', International Journal of Hybrid Information Technology, 9(6), pp. 11–32.

- Feldman, B., Martin, E. M., & Skotnes, T. (2012). Big data in healthcare hype and hope. *October 2012. Dr. Bonnie*, *360*.
- Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future generation computer systems*, *29*(1), 84-106.
- FTS, F. T. S. (2019). Public Cloud vs Private Cloud. from http://www.fiber-optic-transceiver-module.com/will-hybrid-cloud-replace-the-public-private-clouds.html
- Fun, T. S., Samsudin, A., & Zaaba, Z. F. (2017). Enhanced security for public cloud storage with honey encryption. *Advanced Science Letters*, *23*(5), 4232-4235.
- Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137-144.
- Gerner, D. J. (2018). *One land, two peoples: The conflict over Palestine*: Routledge.

The Seybold Report
ISSN 1533-9211

- Ilahi, L., Ghannouchi, S. A., & Martinho, R. (2014). *Healthcare information systems promotion: from an improved management of telemedicine processes to home healthcare processes.* Paper presented at the Proceedings of the Second International Conference on Technological Ecosystems for Enhancing Multiculturality.
- Indu, I., Anand, P. R., & Shaji, S. P. (2016). Secure file sharing mechanism and key management for mobile cloud computing environment. *Indian Journal of Science and Technology, 9*, 1-8.
- Inukollu, V. N., Arsi, S., & Ravuri, S. R. (2014). Security issues associated with big data in cloud computing. *International Journal of Network Security & Its Applications, 6*(3), 45.
- Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A risk management framework for cloud migration decision support. *Journal of Risk and Financial Management, 10*(2), 10.
- Kantarcioglu, M. (2019). *Securing Big Data: New Access Control Challenges and Approaches.* Paper presented at the Proceedings of the 24th ACM Symposium on Access Control Models and Technologies.
- Kaur, P., & Monga, A. A. (2016). Managing Big Data: A Step towards Huge Data Security. *International Journal of Wireless and Microwave Technologies, 6*(2), 10-20. doi: 10.5815/ijwmt.2016.02.02
- Kim, S.-H., Kim, N.-U., & Chung, T.-M. (2013). *Attribute relationship evaluation methodology for big data security.* Paper presented at the 2013 International conference on IT convergence and security (ICITCS).
- Lai, S.-T., & Leu, F.-Y. (2015). *A Security Threats Measurement Model for Reducing Cloud Computing Security Risk.* Paper presented at the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.
- Lim, S. Y., Kiah, M. M., & Ang, T. F. (2017). Security Issues and Future Challenges of Cloud Service Authentication. *Acta Polytechnica Hungarica, 14*(2), 69-89.
- Luong, N. C., Wang, P., Niyato, D., Wen, Y., & Han, Z. (2017). Resource management in cloud networking using economic analysis and pricing models: A survey. *IEEE Communications Surveys & Tutorials, 19*(2), 954-1001.
- Maghrabi, L. A. (2014). *The threats of data security over the Cloud as perceived by experts and university students.* Paper presented at the 2014 World Symposium on Computer Applications & Research (WSCAR).
- Manenti, A., Goyet, C. d. V. d., Reinicke, C., Macdonald, J., & Donald, J. (2016). Report of a field assessment of health conditions in the occupied Palestinian territory
- Mazur, S., Blasch, E., Chen, Y., & Skormin, V. (2011). *Mitigating cloud computing security risks using a self-monitoring defensive scheme.* Paper presented at the Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON).
- McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D., & Barton, D. (2012). Big data:The management revolution. *Harvard Bus Rev, 90*(10), 61-67.

The Seybold Report
ISSN 1533-9211

- Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in hospitals: The application of security safeguards. *Acta informatica medica, 24*(1), 47.
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
- Mengke, Y., Xiaoguang, Z., Jianqiu, Z., & Jianjian, X. (2016). Challenges and solutions of information security issues in the age of big data. *China Communications, 13*(3), 193-202.
- Moje, R., More, P., Soradge, S., & Kakade, R. Design and Implementation of Real Time Embedded Health Monitoring System using Li-Fi technology.
- Named, V. (2008). Cool Vendor" by Leading Analyst Firm, Anonymous. *Business Wire. New York: Apr, 9*.
- NAVYA, T. N., & RAMANJAIAH, G. (2017). Protecting and Verifying Integrity of Cloud Data Regenerating Codes.
- Nyamajeje, B. E., & Yu, H. (2016). *Security for Mobile Application and Its Data Outsourcing in the Cloud Infrastructure.* Paper presented at the Proceedings of the International MultiConference of Engineers and Computer Scientists.
- Pahl, C. (2015). Containerization and the paas cloud. *IEEE Cloud Computing, 2*(3), 24-31.
- PCBS. (2019). The number of Palestinians worldwide has doubled about nine-times.
- Raja, K., & Hanifa, S. M. (2017). *Bigdata driven cloud security: a survey.* Paper presented at the IOP Conference Series: Materials Science and Engineering.
- Ren, Y., Werner, R., Pazzi, N., & Boukerche, A. (2010). Monitoring patients via a secure and mobile healthcare system. *IEEE Wireless Communications, 17*(1), 59-65.
- ResearchGate. (2019). Service Models for Cloud from https://www.researchgate.net/figure/Service-models-for-cloud-computing_fig1_320563162
- Saraladevi, B., Pazhaniraja, N., Paul, P. V., Basha, M. S., & Dhavachelvan, P. (2015). Big Data and Hadoop-A study in security perspective. *Procedia Computer Science, 50*, 596-601.
- Schweiger, A., Sunyaev, A., Leimeister, J., and Krcmar, H. . (2007). *Information systems and healthcare xx: toward seamless healthcare with software agents.* Paper presented at the communications of the association for information systems CAIS.
- Securosis, L. (2012). Securing Big Data: Security Recommendations for Hadoop and NoSQL Environments.
- SHAJAHAN, S., & KHASIM, D. (2017). Guarantying and Verifying Integrity on Multi-Copy Cloud Data.
- Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering, 71*, 28-42.
- Suthaharan, S. (2014). Big data classification: Problems and challenges in network intrusion prediction with machine learning. *ACM SIGMETRICS Performance Evaluation Review, 41*(4), 70-73.
- Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information security in big data: privacy and data mining. *Ieee Access, 2*, 1149-1176.

ISSN 1533-9211

- Yang, S.-J., & Cheng, I.-C. (2015). *Design Issues of Trustworthy Cloud Platform Based on IP Monitoring and File Risk.* Paper presented at the 2015 IEEE Fifth International Conference on Big Data and Cloud Computing.
- Yazan, A., Yong, W., & Raj Kumar, N. (2015). *Big data life cycle: threats and security model.* Paper presented at the 21st Americas conference on information systems.
- Zhang, R., & Liu, L. (2010). *Security models and requirements for healthcare application clouds.* Paper presented at the 2010 IEEE 3rd International Conference on cloud Computing.
- Zhu, H., Zhang, Y., & Sun, Y. (2016). Provably Secure Multi-server Privacy-Protection System Based on Chebyshev Chaotic Maps without Using Symmetric Cryptography. *IJ Network Security, 18*(5), 803-815.