Cloud Data Privacy Preserving Model for Health Information Systems Based on Multi Factor Authentication

Kenneth Gitonga Ntonja, Geoffrey Muchiri Muketha, Gabriel Ndungu Kamau

Abstract- With cloud computing (CC) becoming popular in recent years, variety of institutions, organizations, businesses and individual users are creating interest. They are adopting the technology in order to take advantage of shared web applications, low infrastructure cost, utility and distributed computing, cluster computing as well as reliable IT architecture. In the area of health, Cloud Health Information Systems (CHIS) play a key role not only on the healthcare businesses but patients as well. On the patient side, CHIS aid in sharing of medical data and health information, timely access of critical patient information and coordination of clinical services. Patients, who continue to demand for instantaneous and quality healthcare services are now able to access the services from experts even when they are not necessarily in the same physical location. This is being aided by proliferation of telemedicine through hosted cloud architecture. From the business perspective, CC has helped to cut down operational expenses by way of cost-effective clinical information system infrastructure through the implementation of a distributed platform. The platform has therefore saved businesses millions of dollars that would have gone to infrastructural and human resource investment. Even with these immense opportunities, cloud computing uptake has been serious inhibited by the privacy and security concerns. Due to the sensitivity of personal health information, businesses and individuals are apprehensive when it comes to adopting the technology or releasing the data to the cloud. This study is a results discussion of an enhanced model for attainment of data privacy on the cloud through use of multi factor authentication.

Keywords: Cloud Computing, Health Management Systems, Multi-factor Authentication, One Time Password.

I. INTRODUCTION

Services offered by Cloud Service Providers (CSP) on rental basis can are accessible remotely over the internet. Companies invest a huge amount as a capital expenditure on ICT equipment, services and software. According to Pareto Principle or 80:20 rule, companies invest about 20% of their operating expenses on the core applications for their organizations [1]. In order to increase the operating expenditure and decrease capital expenditure, cloud technology is the most viable choice [2]. Many businesses have adopted the cloud computing as a prime technology for the simple facts like resource sharing, optimal resources utilization, worldwide access, service and platform acquisition cost and many more [3].

In healthcare, Cloud computing is helping in modernization of health services and reduction of cost of doing business. This is being achieved through its ability to facilitate timely information exchange between medical systems and health stakeholders such as patients, doctors and pharmacists. This is particularly practical in instances where medical institutions are distant [3] [4]. Despite these immense benefits, lack of privacy and confidentiality of personal medical data have slowed down the adoption of Cloud Health Information Management Systems (CHIMS). Healthcare data are very sensitive records and should only be accessed by authorized people. However, in emerging technologies like CC where security measures and not standardized, there are possibilities of cyber gaps that pose an adverse impact on the security and privacy of clients' electronic health records [4]. In this regard, security challenges of distributed platforms need to be carefully understood and considered. In recent years there has been a lot of research in an attempt to improve security of cloud-based data. A number of the solutions are based on authentication control mechanisms. Keeping in view the importance of authentication in cloud security, this study proposes an Attribute Based Authentication Model (ABAM) which employs multi factor authentication technique for preservation of privacy of cloud data. The first section illustrates the architectural and function flow design of the model. The last section is a discussion of the results of the survey, model validation exercise and recommendations.

II. RESEARCH METHODOLOGY

A. Research Design

The study design applied was descriptive experimental research (what is going on) approach [4]. The descriptive research was fundamental to proper understanding of the context and how it would apply in the filling of existing gaps. From the findings the inferential statistics will try to determine the cause and effect while descriptive statistics tell what is [5]. The choice of this design was appropriate because involved collection of quantitative data which was tabulated along a continuum in numerical formats and also descriptive data categories regarding the situation based on responses from participants.

Revised Manuscript Received on August 12, 2020.

***** Correspondence Author

Ntonja Kenneth Gitonga, Department of Information Technology, Murang'a University of Technology, Murang'a, Kenya. Email: kengitonga@gmail.com

Geoffrey Muchiri Muketha, Department of Computer Science, Murang'a University of Technology, Murang'a, Kenya. Email: gmuchiri@mut.ac.ke

Gabriel Kamau: Department of Information Technology, Murang'a University of Technology, Murang'a. Email: kamau.gabriel@gmail.com

In essence, why cloud security involved development of casual explanation on why a certain types of security threat were happening more in the Cloud than in traditional computing models. This, therefore, provided an insight on the reasons that may be fueling this trend. The use of descriptive and explanatory research was found appropriate into the research because description helps in uncovering existing gaps within cloud security domain [6]. On the other hand, explanatory research methods give reasons why such challenges are happening [7].

Systematic Literature Review (SLR), experiment as well as survey were the main research methodologies that the study employed. The choice of SLR was to give a summary of the literature related to the study inquiry so as to identify the key words that formed the foundation of the study topic. The keywords were used in Google Scholar, IEEE explore among other university online resources to identify papers related to the research questions. The analyzed literature provided an informed guide in answering the research questions. The literature review was based on published journals as well as other research papers on the research topic.

Choice of survey methodology was essential in designing the questionnaire tool that was be distributed to Cloud users in the selected organization, which was found to use cloud services for some of its core business operations. This, therefore, involved use of random sampling in the identification of an organization as well as individuals who were either using Cloud computing storage services or are planning to do so in the next six months from the onset of the survey exercise. Prepared questionnaires were forwarded to the respondents after a sample population was first ascertained. The questionnaires were distributed through e-mails. For model validation, an experiment was carried out using a demonstration system and trial data.

B. Population and Sampling

This study targeted a population of cloud services users in a health facility that is making use of cloud technology for various internal business operations. Specifically, the research participants were randomly picked from a pool of senior and middle level managers form various departments who included ICT personnel. The sample population was used to analyze and make conclusions on the subject under study. The research used random sampling. This implies that each elementary entity in the sample population had equal probability of being selected for participation in the survey. In selecting participants, Slovin's formula was used. According to Ellen et. al [8] Slovin's formula is employed when nothing regarding the behavior of a population is known at all. In addition, Slovin's formula is useful because it does not require the use of the mean in determining sample size as other formulas require. The formula below is attributed to Michael Slovin [7], [9].

Slovin's Formula:

N/(Ne2 + 1) = n

Where;

e = Confidence Level (percentage)

N = Total target population

n = Sample size

Using the above formula, confidence level can be figured out by research supervisor or the researcher according to the desired expectations. In this study confidence level of e = 0.02 was used, this, therefore, provided level of accuracy of about 98 percent. This was expected to reflect the true picture of the threats within the cloud environment. Using the formula, the population size will be 26 participants selected randomly from a pool of 78 workers.

Thus, applying the formula;

N=78 and e=0.02

n=78/(1+78 * 0.022)

n=78/(1+2.4)

n=26

Therefore, our samplings for this study was 26 respondents. The reason for adoption above formula is to interview a number as close to the total population as possible in order to avoid biases attributed to interviewing few people. Justification for the selections were guided by a number of factors. Firstly, budgetary limitation and logistical challenges could not allow sampling in more than one physical location. Secondly, the target population being a health facility there was the issue of ethical consideration regarding private medical information handled by the facility. Distribution was as follows; ICT 4, Administration 5, Human Resource 5, doctors 6, general line managers 6. Majority of the respondents had moderate knowledge of cloud systems functionality. All except the ICT personnel therefore sought clarification on some of the questions asked. Based on the elaboration, they gave independent responses which informed the conclusions at the end of the study.

C. Data Collection Method and Procedure

For primary data collection the study employed survey method. A survey was conducted using questionnaire tool. The questionnaire consisted of closed and open-ended questions to obtain responses from the respondents. This format made it easier to code, analyze and compare data.

D. Validation Procedure and Participants

The 10-question data collection tool was validated by a team of 5 experts chosen for their knowledge and expertise in cloud security systems. Criteria used by the panel for exclusion or retention of questions included appropriateness for the attribute being measured, clarity of expression, and potential for differentiating the targeted population. Each panelist explained the basis of decision taken to either remove, modify or retain an item. The items which were consistently for removal by at least a third of the panelists eliminated. Similarly, amendments were effected on items that were identified as requiring modification. The final list of items comprised the draft tool that was to be used for data collection. The draft was subjected to the last verification by a smaller team of 3 ICT systems experts. The experts evaluated the level of relevance on a 4-point index (4 = not relevant, 3 = somewhat relevant, 2 = quite relevant, 1 = highly relevant).

The interrater concordance content validity index for items was computed to evaluate validity of the items. Based on the 3-member experts' opinions, 10 items were retained with minimal modifications. Based on these findings the items were good validation of the underlying construct. It was therefore certified that the instrument was acceptable for assessing the opportunities and risks in cloud computing in the target facility. The tool was therefore adopted for assessment of individual perceptions of hindrances that inhibit the uptake and utilization of cloud technology especially in modern health businesses.

E. Data Analysis

According to UNICEF [11], data analysis techniques must be selected to match the specific assessment in terms of its key evaluation questions and the resources available. It goes further to state that the techniques must be able to complement each other's strength and weaknesses, in order to fill the existing gaps with the existing data. For this study, data was analyzed after the first interviews on the information security managers, cloud system users and System administrators.

The study used content data hermeneutics analysis whereby data is done in two ways that is; as fundamental philosophy (concept) and a type of examination [10] [13]. In the philosophical context the use of cloud data threats was driven towards understanding how the system administrators perceived the consequences of security threats, since they were key in supplying answers to our research questions in order to give room for interpretation. On the other hand, a type of examination allowed for understanding the textual data that was collected from respondents. The validity and reliability of the tool were evaluated as follows: Construct validity was established by confirmatory factor analysis and exploratory factor analysis [9]. In our case the sample size obtained from computation method discussed earlier was 26. Therefore, n =26. N was divided into two sub-samples A and B. Exploratory factor analysis was first applied to assess the factor structure of the data collection tool. This was done using the one of the two sub samples that was selected randomly. Bartlett's test for homogeneity of variances and Kaiser–Meyer–Olkin measure of sampling adequacy were used to obtain values for factorization [17]. For tool suitability exploratory factor analysis was used to uncover the underlying variables. For this SPSS 27.0.0 was used. For the interests of discovering the existence of possible trends and patterns in the data, the study employed both measures of spread measures of central tendency. These included frequency, variance, mean and standard deviation. The objective of utilizing these measures was to draw inferences on the attributes under review. For instance, the mean of respondents rating of privacy in the cloud service, mean of subjects understanding of the cloud systems authentication process and mean of subjects subscribing to view of need to improve cloud data privacy through strengthening the authentication process.

The study made a number of generalizations about the populations from which the samples were drawn. In this study, correlation was used to determine association of variables and regression analysis was employed to prove causation relationships between independent variables and dependent variables.

F. Ethical Considerations

Ethical principles were strictly adhered to in this study. Participants were involved in their own volition and given an option to opt out any at given point if they so wished. Raw responses provided by the respondents were treated as confidential. The study ensured that the data analyzed and reported in the research was through openness and honesty. Proper authorization was sought from the facilities where the research data was collected. Full disclosure of findings was shared with the participating individuals and institution.

III. DESIGN OF THE MODEL ATTRIBUTE BASED AUTHENTICATION MODEL (ABAM)

ABAM is an extension of the multifactor authentication model by Prachi [13]. While the Prachi model presented a robust authentication through first and second level authentication checks, it presented multiple unique challenges. First, control of data relied on the CSP. The data owner lacked situational awareness of who was accessing their information and when. Secondly, the model did not provide a comprehensive solution to the problem of encryption of data in transit. Encryption in the Prachi model happens when the data reaches the CSP server. Thirdly, if the data owner loses the mobile phone or there is service provider delay in delivering the secret token, then access to the data is impossible. Further, once the key authentication has been verified, the data requestor has unlimited access to the cloud data. The model did not provide criteria for limiting the type and level of access that the owner transfers to the requestor.

ABAM introduces an encryption mechanism for the data in transit virtually eliminating chances of MiTM attacks [16] [17] [19] [23]. A new security level has been added whereby the data owner classifies cloud stored information in levels depending on confidentiality rating. Read and write permissions are also defined. This way, the data owner retains the authority on who can access their data, level of access and what actions may be carried out on their private data on the cloud. In the Prachi approach, the first step is client registration where user details such as name and valid email address are captured and stored in a database. When a request is received, system generates a key (K). in phase 2 the key (K) goes through a split process to generate k1 and k2. k1 is sent to user mobile while k2 is sent to a registered email. The user responds by keying in the unique key on the interactive portal which is then subjected to a key matching algorithm. The final phase is the access phase. If the keys match the system generated key, user is granted access. Access is denied if the matching criteria is not met. The proposed modification to the Prachi model is illustrated in the ABAM model Figure 1. It shows the expanded functions which are meant to add more security layers to enhance privacy level. The noted weaknesses of the comparison model have been adequately taken care of.

The model uses the legacy password system but goes on to add multiple authentication mechanisms aimed at ensuring the data owner has total control of their cloud data. At the client registration phase, a security feature has been added where read or write rights are defined. Therefore, the administrator can define who has the rights to read and write. For instance, a patient may want to give their personal doctor unlimited access to read and modify their medical records. However, a trusted member of the family may have right to only view the records. Passwords are hashed using SHA2 algorithm and stored in the Cloud Service Provider (CSP) database. There is an elaborate password strength policy which must be met for a user password to be acceptable. When a user successfully gains first level password access, a key (K) is generated.

In the second level of authentication, the model applies a split algorithm to generate k1 and k2 from key (K). k1 and k2 are sent to the registered email and mobile. The user must acknowledge by way of replying using the unique key which is in the form of a random system generated 6-charcater One Time Password (OTP). Once the OTP is received, it is subjected to an algorithm to ascertain that it matches the original key and secondly, it is from a valid mobile number of email address. Integration of the OTP verification process is aimed at preventing man in the middle attacks. It therefore means that the system will deny access if the OTP is received from a mobile number or email that is not recognized. Finally, the model provides an audit mechanism through generation of logs for every activity that includes a time stamp. The file has an option for archiving or export to email.

ABAM is designed on client-server model and founded on the virtualization hypervisor. The model utilizes Type 2 hypervisor within the PaaS and SaaS [23] [24] [27]. The Graphic User Interface (GUI) is hosted on application layer of OSI model. Fig. 1 illustrates the general overview of the model functionalities. The model application server and database is embedded within the PaaS layer of the cloud infrastructure. For SMS and mail notification, the model employs Infobip platform which integrated seamlessly with the model through use of Java and PHP programming languages [12] [14]. The messaging gateway services was acquired from Safaricom, which also provided the unique sender ID. This featured added to the layered security implementation strategy. As a result, adequate security and practical efficiency in the cloud storage was achieved as expected.

ABAM is a modular architecture with key units being; Administrator module where the admin can add, delete and define user rights and access levels, User interaction module or the Graphical User Interface (GUI) and encryption/decryption module. This is where encryption and decryption using mcrypt algorithm takes place.

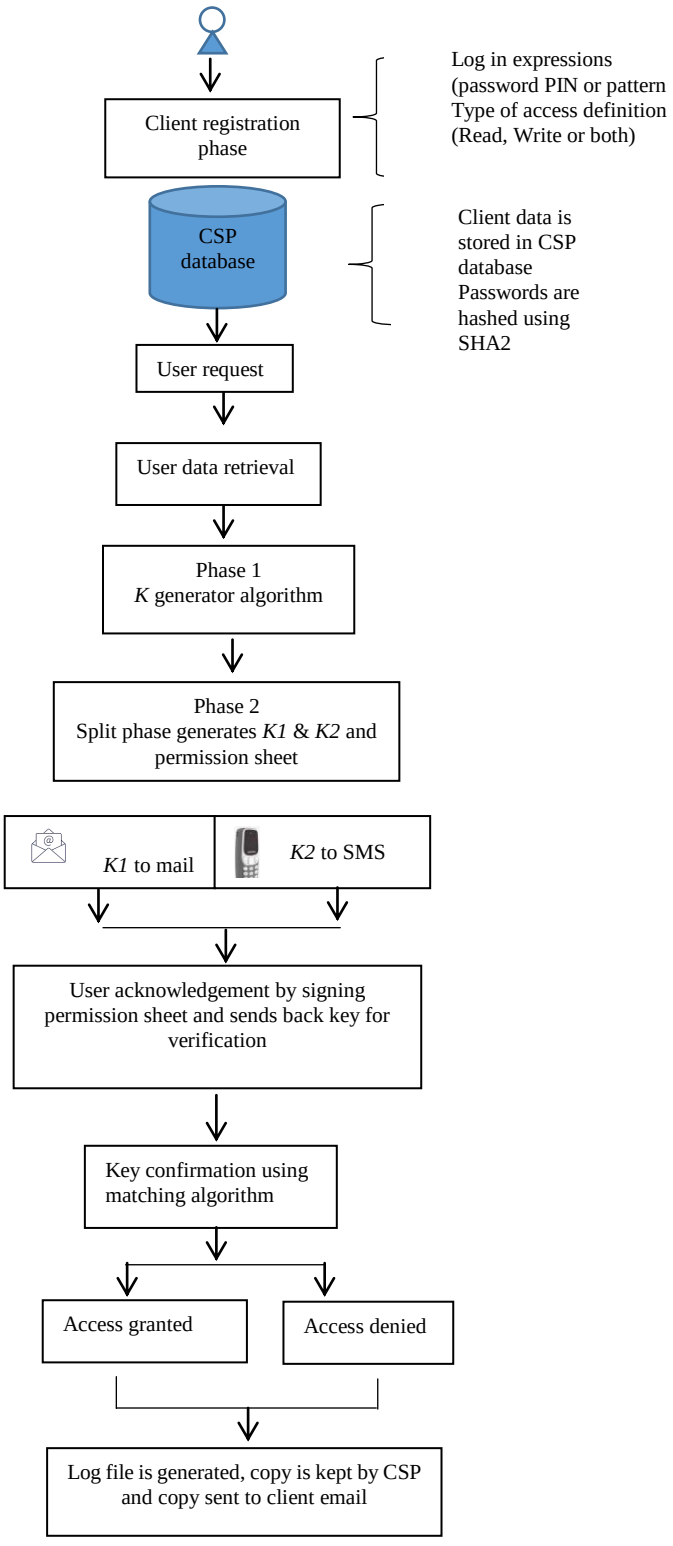

Fig 1. The ABAM model

A. Model Activity Flow Chart

The flow of processes in the proposed ABAM model is shown in Fig 2.

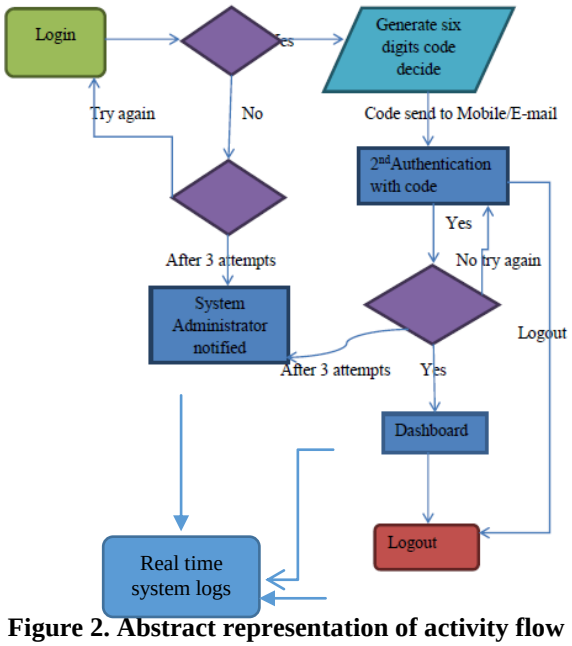

Figure 2. Abstract representation of activity flow

B. ABAM Interface Design

Interface design determines the usability of an application. In designing the interface, careful consideration was made to ensure the attributes of usability and understandability are attained.

1). User Registration

Client uses the electronic form to register with the cloud application. Details required are a valid email address and a password that meets the set security policy.

2). User Login

Client uses login portal to request access. User then submits the credentials for first level authentication check.

3). Key generation

Once the first-round authentication is successful, system generates a random Key (K) which is a unique set of 6-character code that changes randomly with every attempt.

4). Key Split

The key (K) is split into k1 and k2 which both of which are identical. The keys are then automatically sent to user mail (k1) and mobile phone (k2)

5). Zero Knowledge Proof Protocol

Zero-knowledge proof is a protocol whereby data is shared between party A usually referred to as the prover and B, called the verifier without requirement of a password or any other credentials. Zero Knowledge Proof Protocol virtually eliminates the possibility of a Man in the Middle attack because there is no exchange of authentication credentials. [17] [19]. In ZKP a client picks a random value y, and computes d, where d = mod p. The computed d is then sent to the cloud service provider. When the cloud service provider receives d, it replies by sending back a random challenge x to the client from which the request originated. Upon receipt, the client computes u and v where, u = y+xm (mod q) and v =s+xr (mod q). v and u are then sent back to the cloud service provider. If the cloud service provider validates v and u, then zero knowledge proof is successful and therefore the client is granted access to the database as illustrated by the flow diagram in Fig 2.

C. ABAM Algorithm

The sequence of processes in the ABAM model are as follows. A client registers via an electronic registration form. Password is stored in SQL database in hashed form using SHA-2. When a login request is made, the system sends the authentication credentials to the Identity provider where the credentials are matched with the stored authentication data. In case of successful login, the split key generator using elliptic curve point generation produces Key 1 and Key 2 (k1 and k2) which are sent to a preregistered mobile number and email respectively. Client responds to the notification which is sent back to the identity provider for second round of authentication confirmation. If the notification is not received or it is delayed for a given time limit, access will not be granted even if the first credentials were authentic. An access log is created with a time stamp for every successful or failed attempt.

D. Elliptic Curve Points Creation for OTP Generation

Elliptic curve generation over real numbers is a set of points (x,y) which must mathematically satisfy the elliptic curve equation $y^2 = x^3 + ax + b$, in this case a, b, x, y must be real numbers.

E. Encryption Process

On the elliptic curve, select a random point *P*. generate cipher text by computing a pair of points on the curve

1). Calculate *r* (where r is a random number) and when, whereas m is an identity attribute

2). *f* and *g* will be the generators of point h on the elliptic curve.

3). Using the above, compute *K* which is a product of the attributes defined above denoted as attributes *n*.

4). Now compute μ which is a product of the attributes *n*

5). K is now split into 2 parts *k1* and *k2*. *k1*value is sent to mobile through SMS and *k2* is sent to a registered email.

6). The next phase is the zero-knowledge proof where whereby the ZKP steps discussed earlier are executed for the CSP to grant the client access to the desired information.

IV. IMPLEMENTANTATION OF THE ABAM PROTOTYPE

This section is an illustration of an interactive front-end tool developed to demonstrate the functioning of the proposed ABAM model Using the tool users were created and rights assigned. The data was hosted on the cloud at Skydatalabs. Skydatalabs is a company that offers IaaS for cloud hosting. Fig 3. Shows the login GUI where the user enters their valid email address as registered during initial user creation process. The password must meet the complexity criteria that is set in the password policy. Wrong credentials will trigger a login failure message as shown in Figures 4 and 5. User login information is validated by comparing the details already saved in the users' database. If they match, the first round of authentication is confirmed and a six character OTP sent to the registered mobile phone as illustrated in Fig 6. The user must provide the OTP for second round of authentication. Third level authentication involves verification of the OTP through a matching algorithm.

The interactive portal illustrated has been designed in

consideration of the targeted users of the model. It is an easy GUI that would not pose any challenge even to the least technical users. The administrator has the privilege to add users, delete or modify details. Normal users have rights to only read information. The right to modify information is reserved to the administrator and the data owner only.

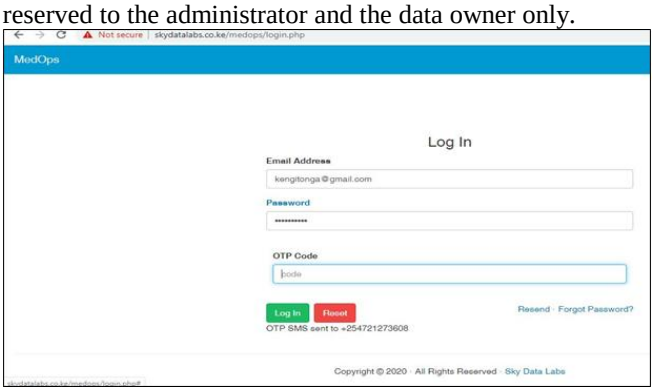

Fig 3. Interactive log in portal

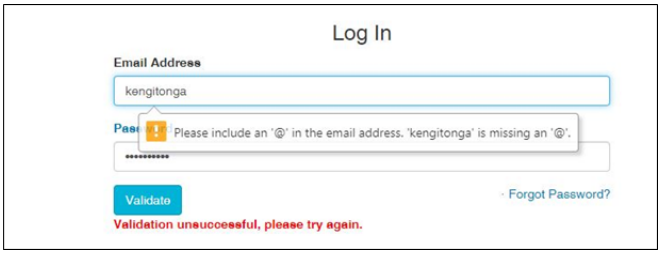

Fig 4. Error alert on wrong email

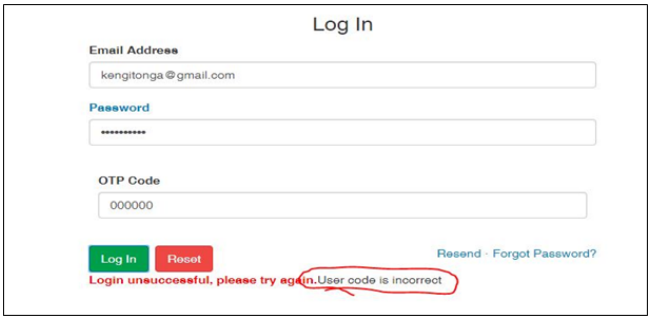

Fig 5. Error alert on entering wrong OTP

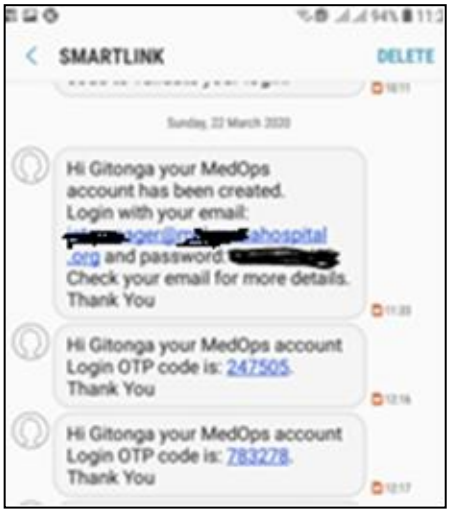

Fig 6. Mobile OTP alert

V. RESULTS

A survey was carried out in Maua Methodist Hospital in Meru County, Kenya. The facility cloud technology for its core health system as well as other support services. It involved senior and middle level managers. Justification for this is because the middle and higher-level managers have a better understanding of technology application in organizational operations. They are also the decision makers in matters regarding uptake and investment in emerging technological trends. A total of 31 online questionnaires were sent out and 26 responses were received representing 83.9% response rate. Data analysis and reporting was done using Survey Monkey Analyzer *https://www.surveymonkey.com* – a free online based research data collection, analysis and reporting tool. The aim of the survey was to assess the threats and opportunities of cloud computing specifically in health care industry. It further sought to find out why in general the adoption of cloud technology in the health sector is low compared to other businesses. The findings of the survey would then justify the relevance and urgency of the study. The following are the summarized outcomes of the survey.

a) Which of these cloud services is your health facility using?

The question was aimed at assessing the type of cloud services that the organization is utilizing. The fact that 6 respondents (16%) said they are not sure indicated that some of the managers lacked deeper understanding of cloud deployment models. This could partially explain why cloud utilization in such a facility is still very low hence maximum benefits cannot be drawn from the technology. The outcomes are illustrated in Table 1.

Cloud Platform in use	% of respondents
SaaS	32
PaaS	30
IaaS	22
Not sure	16

Table 1. Cloud Models in use

b) What kind of business processes does your health facility run on cloud services?

A total of 25 responses were returned to this question. Out of these, 68% opined that the facility is using cloud technology for its core health management systems. The lowest adoption is in management support systems where only 3 (9%) said the facility is utilizing cloud-based platform as at the time of the survey as shown in Table 2.

Processes Running on Cloud	% of respondents
Key processes	68
Support services	23
Management processes	9

Table 2. Processes running on cloud

c) To what extent do you agree that the following factors influence the adoption of cloud services in your health facility? Use the following Likert scale to rate your level of agreement that cloud adoption is driven by the following factors.

This question formed the basis of the study which is aimed at addressing privacy issues in cloud-based systems. It was aimed at finding out the reasons why businesses are not rapidly taking up cloud technology. As shown by the responses scalability was the least inhibiting factor at 8%. 11% felt that cost was a major determinant. The biggest number of respondents (69%) strongly agreed that privacy was the main reason that has influenced adoption of cloud technology as illustrated in Table 3.

Factors influencing Cloud Uptake	% of respondents
Privacy	69
Availability	12
Cost	11
Scalability	8

Table 3. Factors influencing cloud computing uptake

VI. DISCUSSION

Various businesses and organizations are rapidly developing their Information Processing Systems (IPS). However, they are still at the beginning of a transition process. Many challenges will be encountered during the process of transitioning from legacy systems to cloud platforms. In healthcare sector, adoption of cloud technology remains very low compared to other businesses. One challenge that has contributed to this phenomenon is the one to do with privacy of personal health data. This study was aimed at proposing a model for enhancement of privacy of data for use in health systems. The idea is however applicable in any other business area. Through systematic review of literature, the study uncovered a serious need for further development and improvement of the existing security models in order to come up with stronger privacy preserving mechanisms for health systems running on the cloud. The study went deeper into exploring the correlation of health data privacy concerns and the rate of individuals' acceptance of cloud health systems. Based on validated findings, it can be concluded that perceived benefits and patient information privacy concerns have a direct impact on individuals' as well organizational acceptance of cloud technology. Even with this inference, it was observed that personal interest also played a key role. The study also explored the effect of regulatory policies on attainment of privacy needs in cloud-based health systems. On policy, the study was keen to find out the platform users' level of awareness on the role of policy regulations and if policies have an impact on the decision of cloud technology acquisition.

The study findings showed that regulatory factors play a key role especially in organizations that are directly under control of the government. The study further revealed that potential cloud users agree that stronger privacy models and assurance of confidentiality of data on the cloud can result in increased adoption of cloud health platforms. The research work led to important practical as well as theoretical inferences. The findings provided a theoretical framework to explore the role that privacy fears have on the rate of acceptability of health systems based on cloud technology. The common observation from the study findings is the universal consensus for further improvements of privacy mechanisms for cloud hosted health data. The study further identified the need for trust building actions among potential users of health cloud systems. Despite the outlined user concerns, it is also agreeable that a higher level of acceptance can be ensured through concerted efforts aimed at convincing businesses of the benefits of investing in the technology. For personal medical records that may be classified as sensitive, the utilization of the proposed ABAM solution would lead to higher approval of cloud-based health systems.

VII. CONCLUSION

Cloud Computing is a paradigm which if well utilized can deliver many benefits to modern day businesses. In healthcare, the technology can transform health services delivery hence benefiting both the healthcare providers and patients. The study reviewed how privacy has a direct correlation on the user confidence in the cloud technology. On the process, it unveiled limitations which would be possible avenues for future studies. First, future studies should investigate other emerging models and review their privacy preservation approaches with a view of identifying possible gaps before they are adopted in the market. Researchers should put more emphasis at measuring other attributes related to cloud data privacy fears. A deeper analysis of the role of government regulation on the implementation of security systems could also lead to vital contributions on this topic. Trust building measures obviously will play a major role in the rate of acceptance of the cloud systems. This therefore offers and exciting area that researchers can investigate with an aim to establish methods that can be applied to boost user trust.

Finally, although the study was conducted with health care systems in focus, it would be interesting to explore the platforms being used in other forms of businesses and how confidentiality is being attained with an aim of replicating the same strategies in healthcare systems in future system development projects.

In conclusion, cloud computing technology is still a young technology in healthcare. If researchers can find ways of combining it with other emerging technologies like Internet of tings (IOT), Big Data Analytics (BDA) and Artificial Intelligence (AI), many more benefits can be derived with the core objective of improving efficiency as well as opening up new avenues for quality healthcare services delivery. Besides these, CC improves interoperability of software and infrastructure, boosts resources availability and greatly reduces operation costs. With all these advantages and the widespread research already taking place to address data privacy and confidentiality challenges there is no reason why healthcare businesses should not migrate to cloud.

REFERENCES

1. Bajwa, M. S., Himani, & Sandeep, S. K. H. (2015). An Enhanced Data OwnerCentric Model for Ensuring Data Security in Cloud. 2015 Second InternationalConference on Advances in Computing and Communication Engineering
2. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1,no. 1, pp. 11–33, 2004.
3. Hyokyung Chang and Euiin Choi, "User Authentication in Cloud Computing", Springer-Verlag Berlin Heidelberg 2011, UCMA 2011, Part II, CCIS 151, pp. 338–342.

4. Baliga, P. Kamat, and L. Iftode, “Lurking in the Shadows: Identifying Systemic Threats to Kernel Data (Short Paper),” in 2007 IEEE Symposium on Security and Privacy, May 2007.
5. Jiangshan Yu, Guilin Wang, Yi Mu, and Wei Gao, "An Efficient Generic Framework for Three-Factor Authentication with Provably Secure Instantiation", IEEE, 2013
6. Behl, “Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation,” in Proceedings of the World Congress on Information and Communication Technologies (WICT ’11), pp. 217–222, IEEE, December 2011.
7. Pandey, R. M. Tugnayat, and A. K. Tiwari, “Data Security Framework for Cloud Computing Networks,” International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178–181, 2013.
8. A.Ibrahim, B.Mahmood and M.Singhal, A secure framework for sharing electronic health records over clouds, in Proc. of IEEE International Conference on Serious Games and Applications for Health (SeGAH), pp. 1-8, 2016.
9. Amir, M. T., Rodziah, T., Rusli, A. & Masrah, A. A. M. (2012). Security Frameworkof Cloud Data Storage Based on Multi Agent System Architecture – A Pilot Study.
10. Shirly Lee, Tae Yong Kim and Hoon-Jae Lee, "Mutual Authentication Scheme for Cloud Computing", Future Information Communication Technology and Applications, Springer, chapter 17, 2013, pp 149-157.
11. PrachiSoni and MonaliSahoo, "Multi-factor Authentication Security Framework in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, ISSN: 2277 128X, January 2015
12. Arockiam L. and Monikandan S., Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. International Journal of Advanced Research in Computer and Communication Engineering, 2(8), pp.3064-3070, 2013.
13. Bartock, M. et al. (2015). Trusted Geolocation in the Cloud: Proof of ConceptImplementation.National Institute of Standards and Technology.Beal, V. (2015).Data. http://www.webopedia.com/TERM/D/data.html. Accessed 20.09.2018.
14. E. Keller, J. Szefer, J. Rexford, and R. B. Lee, “NoHype: virtualized cloud infrastructure without the virtualization,” in Proc. 37th annual international symposium on Computer architecture, New York, NY, USA, 2010, pp. 350-361.
15. F. Monrose, P. Wycko, and A. D. Rubin, “Distributed execution with remote audit,” In NDSS, 1999.
16. Keramidas, A. Antonopoulos, D. N. Serpanos, and S. Kaxiras, “Non deterministic caches: A simple and effective defense against side channel attacks,” Design Automation for Embedded Systems, 12(3):221-230, 2008.
17. G. Kumaresan, N. Veeraragavan, Dr. L. Arockiam, "A Study of User Authentication Techniques in Cloud Computing", Journal of Emerging Technologies and Innovative Research (JETIR) (ISSN-2349-5162), Volume 2, Issue 8, August 2015, pp. 3309-3314.
18. HyosikAhn, Hyokyung Chang, Changbok Jang, and Euiin Choi, “User Authentication Platform Using Provisioning in Cloud Computing Environment”, Springer-Verlag Berlin Heidelberg 2011, ACN 2011, CCIS 199, pp. 132–138.
19. Kong, O. Aciicmez, J.-P. Seifert, and H. Zhou, “Deconstructing new cache designs for thwarting software cache-based side channel attacks, In 2nd ACM Workshop on Computer Security Architectures, pages 25-34, October 2008.
20. Szefer, E. Keller, R. B. Lee, and J. Rexford, “Eliminating the hypervisor attack surface for a more secure cloud,” in Proc. 18th ACM conference on Computer and communications security, New York, NY, USA, 2011, pp. 401-412..
21. Benson, R. Dowsley, and H. Shacham, “Do you know where your cloud files are?,” in Proc. 3rd ACM workshop on Cloud computing security workshop, New York, NY, USA, 2011, pp. 73-82.
22. Suzaki, K. Iijima, T. Yagi, and C. Artho, “Memory deduplication as a threat to the guest OS,” in Proc. Fourth European Workshop on System Security, New York, NY, USA, 2011, p. 1:1-1:6.
23. Blanton, Y. Zhang, and K. B. Frikken, “Secure and Verifiable Outsourcing of Large-Scale Biometric Computations,” in Privacy, Security, Risk and Trust (PASSAT), IEEE Third International Conference on Social Computing (SocialCom), 2011, pp. 1185-1191.
24. J. Atallah and K. B. Frikken, “Securely outsourcing linear algebra computations,” In ASIACCS, 2010.
25. M. Y. A. Younis and K. Kifayat, “Secure cloud computing for critical infrastructure: a survey,” Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.
26. Michael E.Whitman In defense of the realm: Understanding the threats to information security International Journal of Information Management, 24, 2004, pp.43-57.
27. Nan Chen and Rui Jiang, "Security Analysis and Improvement of User Authentication Framework for Cloud Computing", Journal of Networks, Vol. 9, No. 1, January 2014, Pp 198-203.
28. Rohitash Kumar Banyal, Pragya Jain and Vijendra Kumar Jain, "Multi-factor Authentication Framework for Cloud Computing", IEEE Computer Society, Fifth International Conference on Computational Intelligence, Modelling and Simulation, pp 105-110.

AUTHORS PROFILE

Kenneth Gitonga Ntonja is currently the ICT Manager in Maua Methodist Hospital, Kenya. He has over 10 years’ experience in planning, installation and administration of Health Management Information Systems (HMIS). He received his BSc in Information Technology from Meru University of Science and Technology (Kenya) and is currently pursuing his MSC in Information Technology from Murang’a University of Technology (Kenya). His research interest includes Health Information Systems security and Cloud Systems Security (CSS).

Geoffrey Muchiri Muketha is an Associate Professor and Dean School of Computing and Information Technology, Murang' a University of Technology, Kenya. He received his BSc. in Information Science from Moi University, his MSc. in Computer Science from Periyar University, and his Ph.D. in Software Engineering from Universiti Putra Malaysia. His research interests include software and business process metrics, software quality, verification and validation, empirical methods in software engineering, and component-based software engineering. He is a Professional Member of the ACM and a member of the International Association of Engineers (IAENG).

Gabriel Ndung’u Kamau is lecturer of Information Systems. He has over 14 years of work experience in Information systems, research and consultancy, and educational development. He has a PhD in Business Administration in the area of Strategic Information System and Master of Business Administration (Management Information Systems) from University of Nairobi.

He has vast knowledge and experience in Management Information Systems, Information Security and Applied Cryptography, Computer Forensics, Enterprise Risk Management of Information Systems, Information Security Audit and IT Governance. His Current research interest include Computers Security, ICT4D, Data analytics and research in Information of Science Philosophy Perspectives.