The Use of Biometrics in Multifactor Authentication (MFA) for Cloud Computing Data Storage

Lavender A. Ochiel
School of Computing and Informatics
University of Nairobi, Nairobi, Kenya

Elisha O. Abade
School of Computing and Informatics
University of Nairobi, Nairobi, Kenya

ABSTRACT
Cloud Computing can be defined as a technology that allows access to computing resources and services in a flexible, scalable and highly available manner over the internet. It has been gaining momentum over the years with several organizations targeting cloud migration from the conventional on-premise approach for their data centers. Cloud Service Model offerings such as Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) has grown in adoption with cloud data storage being one of the popularly used services in the public cloud. With the widespread growth of cloud computing services, new security and privacy issues have arisen, posing an open challenge to adoption of the cloud computing paradigm. Authentication stands to play an important role in mitigating the security and privacy issues foreseen. There is a need to enhance the current authentication schemes in use which are known to be prone to security threats and attacks. Multi-factor authentication allows the use of more than one authentication factor; knowledge, possession and inherence with combinations of the first two currently being used by most cloud service providers however still facing security breaches. In this paper, the author discusses security threats in cloud computing, the current multifactor authentication mechanisms in use and how to enhance multifactor authentication using fingerprint biometrics in cloud computing data storage to assure confidentiality and integrity of user data.

General Terms
Minutiae Algorithm, Fingerprint Enrollment, Fingerprint Matching, APIs.

Keywords
Biometric, Multifactor Authentication, Fingerprint Scanning, Cloud Computing

1. INTRODUCTION
Cloud Computing (CC) has been gathering momentum over the past few years with many businesses, organizations and individuals taking it up. It employs the use of services that are paid for per-use to setup computing infrastructure or utilize services in an efficient, costly, available and reliable manner over the Internet. Even though cloud computing comes with benefits, concerns of data security in the cloud has been the main barrier to its widespread use [1].

The major security issue on cloud computing is protecting data and applications from unauthorized access. Traditional authentication schemes currently adopting main technologies of authentication factors which are **knowledge factors** (what a user knows), and **possession factors** (what a user has) have been used to restrict access to cloud services. The drawback with this authentication scheme is that security can easily be compromised or breached when passwords or PINs are revealed to unauthorized users.

Multifactor authentication using Biometrics whose authentication scheme is categorized as an **inherence factor** (what a user is) in combination with the existing authentication of knowledge and possession factors can serve to address the problems posed by the challenges inherent from traditional authentication techniques based on single factor.

Security being a major concern for users, cloud providers and data hosted on cloud platforms. There is need to incorporate more than one authentication factor to add an extra security layer to systems. Cloud service providers like Amazon Web Services use multifactor authentication that combines knowledge factors (username and password) and possession factors (MFA device) to add the extra layer of security in accessing the cloud services [2]. However, possesion factors still have a drawback in that they can be stolen or can get lost and land in the hands of wrong people who might attempt to use them inappropriately.There is therefore a need to incorporate inherence factors (Biometrics) to ensure that authentication for clouds data services access is guaranteed without leaving loopholes for attacks or threats [3].

The rest of this paper is organized as follows: section 2 provides a literature review about and related work . Section 3 and 4 respectively, present methodology used and results & discussion of the research. The conclusion is provided in section 5.

2. LITERATURE REVIEW
With the growing popularity of cloud computing, security threat has been found to be the major hinderance in increasing cloud computing growth [4]. In this section, this paper discusses cloud computing paradigm, security issues in Cloud Computing, relevant works that have carried out to address the eminent security issues and how to incorporate biometrics in cloud computing.

2.1 Security Challenges in Cloud Computing
Security and privacy issues are a challenge in cloud computing that is quickly gaining popularity. This is due to cloud computing's multitenancy nature as well as outsourcing of applications that are critical, sensitive data and infrastructure [5]. With all the control of the data premises sitting with the cloud services providers, the information owner is concerned over the risk of data loss when they relinquish control of processing information to the cloud [6]. Cloud Security Alliance's Treacherous 12 Working Group Conducted research to identify the top security threats in cloud computing to aid users and service providers in making informed decisions when it comes to cloud computing. In their report that was published in 2016, they narrowed down the list to top 12 threats that require attention [7]. Berry, [8] indicates in his article how in July 2015, PagerDuty, a

company dealing with operations performance management advised their customers to alter their credentials (usernames and passwords) after finding out that their systems had been breached. An attacker had gained access to PagerDuty servers' through Linode's [cite] administrative panel by by-passing the two factor authentication controls. Even though Linode had implemented Time-based One-time Password (TOTP) and username and password, the attackers gained access to one of the employee's credentials and used them to access the control interface, thus bypassing the MFA system resulting in a security breach. As a result, PageDuty moved its services to another cloud service provider causing Linode to lose business. This is clear evidence of the security threats that are prevalent even with MFA involving knowledge and possession factors creating a gap that needs to be addressed. Whereas OTP passwords was incorporated in Linode's systems, the attackers still managed to steal credentials and access the system. Incorporating biometrics would resolve such issues hence the need for further research and work in this regard. Another major threat in cloud computing authentication is account hijacking where an attacker gains unauthorized access to client's details and uses them to access their cloud services. Once a hijacking is successful, an attacker eavesdrops on authorized user activities, poses as that user and interferes with the network data or uses the credentials for malware propagation for instance redirecting users to malicious websites. These threats are quite like those in the conventional computing environments [1].

2.2 Related Work

2.2.1 Multifactor Authentication for Cloud Computing

Veerendra and Prasad, [9] in their paper, explored the current security challenges in cloud computing authentication and considered more than one knowledge factors including username, password and color value for authenticating users. They came up with a system that in addition to the two authentication factors gives the user the liberty to choose the encryption algorithm from the ones configured like DES, AES, blowfish and recursive key generation. Whereas these encryption options further hardened the system, the end users would not have been well informed to know which one of them to go for. It would rather have been efficient to choose the encryption algorithm with the most efficiency for this kind of system and have it run in the background without the end user's knowledge. Their system involved a two-step process with a registration and login phase. Registration involved recording of username, password and chosen color which was stored in the database while login phase involved retrieval of the saved credentials to allow access. In addition to the multifactor authentication, they used hash algorithms to encrypt and secure data in the business premises and not on the cloud, thus enhancing security. However, with their prime focus on keeping the data on premises, they really did not address the concern of authentication to ensure stored cloud data integrity and confidentiality.

Considering their approach focused only on knowledge factors though they incorporated more than one, it would still leave loopholes for a brute-force attack as an attacker can use trial and error to figure out the color that a user has set to use in authentication. Therefore, the addition of a second option of the same mode of authentication could enhances security but a more viable approach would still be feasible to ensure such attacks on knowledge factors do not comprise users access to their cloud resources by ensuring the user is the rightful person they purport to be and not otherwise.

According to Amazon Web Services [2], AWS, one of the giant cloud service providers recognizes Multi Factor authentication as an industry recognized best practice when it comes to securing cloud access since it adds an extra layer of security on top of conventional username and password. They put place mechanisms that enables the users to set up knowledge (username and password) factors as a first level of authentication and enhance it by possession factors that is having the user provide an authentication code from an MFA enabled device. This is applicable for AWS account, individual accounts on Identity Access Manager (IAM) as well as AWS Service APIs. The available options for MFA include One Time Passwords, Hardware and Virtual MFA enabled devices as well as SMS authentication. These multiple factors provide increased security for a user's AWS account settings and resources [2]. It's a good initiative considering the industry hype for the cloud service providers to embrace MFA but it's evident that most of the focus is on possession factors. The only challenge with this is that when a user loses the MFA enabled device then the risk of their credentials getting compromised is high. Among the options shared by AWS, there isn't a single inherence factor that is available for use. This calls for the need to assess and analyze inclusion of inherence factors (what a user is) to enhance security and address the issue of potential loss of possession factors. It would also be vital to establish why Cloud Computing providers have not incorporated biometrics to MFA for example.

Soni, P et al [6] proposed a Security framework for Cloud Computing Data security. They looked at various aspects to ensure that only the owner of the data in the cloud can gain access to the data and ensuring that even the cloud service cannot view the data in a bid to ensure confidentiality and integrity of the data. They came up with a framework that infused authentication and authorization, access control based on attributes as well as data integrity and confidentiality. For authentication and authorization, they proposed a framework with MFA that includes knowledge factors (username and password) as a first step of authentication and possession factors in the form of a unique key that would be generated, split into two; key 1(k1) and key2 (k2) and sent to email and mobile phone respectively for confirmation before access could be granted. It's however not clearly defined how the key would be encrypted to ensure that it's not compromised during transmission to the MFA device. Like any other possession factor, there would still be room for authentication compromise in cases where the phone or email account gets hacked resulting into the wrong person gaining access to the system and accessing the user data whose security is the major target in this research paper. Incorporating inherence factors in MFA would assure confidentiality and integrity of the data as what a user is for example finger biometrics would ensure that there is less probability of loss as in the case of MFA devices.

Panse and Haritha [5] in their paper indicated that with the flexibility that comes with Cloud Computing and the increased adoption, the major challenge that needs to be addressed is security because of cloud computing's multitenancy nature, outsourcing of infrastructure, sensitive data and critical application. Additionally, provision of physical security controls in the cloud environment is next to impossible. They discussed the different authentication methods and the need to incorporate multiple factors for authentication to secure cloud data. Conventional methods that have been used individually in authentication include; digital signature, passwords and PIN, symmetric and public

key cryptography, SMS based, and biometric authentication as well as zero knowledge proofs. However, they proposed the use of more than one factor authentication and further discussed the various MFA categories; possession factors (what a user has), knowledge factors (what a user knows) and inherence factors (what a user is). Multifactor raises the threshold for attacks because the masquerading attacker would need to crack more than one level of authentication to compromise the cloud environment and gain access to the cloud data [5]. Even though their study clearly outlines the need for MFA in cloud computing, there is no clear approach as to how to tackle confidentiality, integrity, availability and anonymity using the proposed authentication methods to secure data in the cloud.

2.2.2 Biometrics in Multifactor Authentication for Cloud Computing

Biometric authentication is the use of physical or behavioral factors to identify users are who they purport to be. These include fingerprint, iris, face, palm veins, voice, keystroke, signature and DNA. Whereas on one hand each of the factors has an advantage tied to it, there is an associated disadvantage on the other hand. Naveed et al, [10] in their paper explored the different biometric authentication factors that can be employed in cloud computing authentication, their advantages and drawbacks. They reiterated that the use of fingerprint recognition in biometrics was a well-known and widely used technique because it is easy to use and generally acceptable in very part of the world. Whereas fingerprint scans had a very low error rate and have been used for several years, their accuracy could be affected by cases where the finger was dirty or damaged. Iris scans were quite accurate and reliable however users could be skeptical to expose their eyes to light from the scanning machines. Facial recognition was simple and could be widely accepted by users but very low on accuracy due to the changing facial expression. Finally of the factors they discussed, retina can be very liable with very low error rated however users may exhibit phobia to exposing their eyes to light. They therefore suggested the use multimodal that is more than one biometric factor in authenticating users in the cloud. However, due to the cost implication, implementation challenges and availability of the sophisticated devices required to facilitate biometric authentication, it might not be very easy to roll out more than one mode hence the need to infuse biometric with other factors like knowledge or possessions factors to add extra layers of security in cloud computing authentication.

Qaddour [11] proposed the use of multifactor biometrics authentication for cloud computing. This involved knowledge factors (username & password), a True Random Number Generator (TRNG) with values of one to four and more than one inherence factor including facial recognition, voice recognition, fingerprint and iris scan. An algorithm that allowed for registration of users by collecting the biometric data for all four modes and storing the details in specific templates was proposed. On access request, a user would login with username and password after which a TRNG would generate a random number. Each of the biometric modes would be tagged to the numbers 1 to 4 and the corresponding template would be fetched based on the randomly generated number. The user would then be prompted to input the details; facial or voice recognition, iris or fingerprint scan and full access grant when a match was detected. Whereas this seems to be addressing the security issues in cloud authentication, there would be a need to get highly sophisticated devices and corresponding software to be able to register and use the four biometric modes all together. This would prove to be a very expensive implementation hence the need to find better and more efficient options to secure the cloud data.

Choudhari and Bodhe [12] in their paper proposed the use of thumb print scanning as means of authentication for cloud services. This would be used as a replacement for the traditional username and passwords that are prone security attacks due to the different hacking techniques that are available. They proposed a biometric modal system that would perform three major steps as far as thumb print authentication is concerned; pre-processing stage where the fingerprint print artifacts were extracted, enhanced to remove background noise for example and normalization of the same. The second stage was the template generator that would extract the scanned print and produce a template. Finally, to store the template in a biometric database marking the end of enrollment. During login, a user thumbprint template generated at that point would be checked against those that existed in the database and if there was a match, access was granted. This was indeed a more secure option as compared to username and password login, however, this paper doesn't detail the algorithms that would be used for fingerprint processing, system components or further studies on the use of the proposed biometrics. The focus here as well is still on a single authentication factor yet there have been recommendations to embrace Multiple factors to beef up security in cloud computing. MFA is the best practice that adds another layer of security on top of traditional username and password [2]. There is still room for further work to incorporate other authentication factors together with the proposed biometrics to enhance security while accessing cloud data storage services.

Sanya et al. [13] proposed the use of biometrics in cloud computing in the research they conducted to secure data storage and sharing in the cloud. According to them the use knowledge factors i.e. usernames and passwords is becoming hectic for users as they must remember several such pairs of credentials that may lead to them forgetting the same, hence biometrics is a possible solution. Even though biometrics have been widely used on private setups to secure data, it hasn't been used as much in the case of internet usage where the cloud resides. This has been due to the accessibility and scalability of biometric technology. In their work, they proposed a multimodal biometric system comprising of fingerprint scan and iris authentication that incorporated the use of encryption keys as well to authenticate cloud service users. The logic involved a user getting an encryption key from the admin as a first step to authentication, then using fingerprint scan and finally iris scan before access could be granted to a cloud service. Whereas they discussed the use minutiae algorithm used in fingerprint scanning, it is not clear how the system architecture was and whether the biometric authentication was happening locally or in the cloud. There was also no clarity on what services in the cloud were being accessed and whether their proposal addressed other security metrics apart from authentication. Therefore, as indicated to perform further work on multimodal biometrics part of which is already discussed in this paper (iris and fingerprint scan), there is a need to further investigate how confidentiality and integrity can be assured through the incorporation of biometrics in cloud computing.

2.3 Conceptual Design

The conceptual design in this research involved the use of biometrics and username/password to authenticate cloud storage users as illustrated in the **figure 1** below.

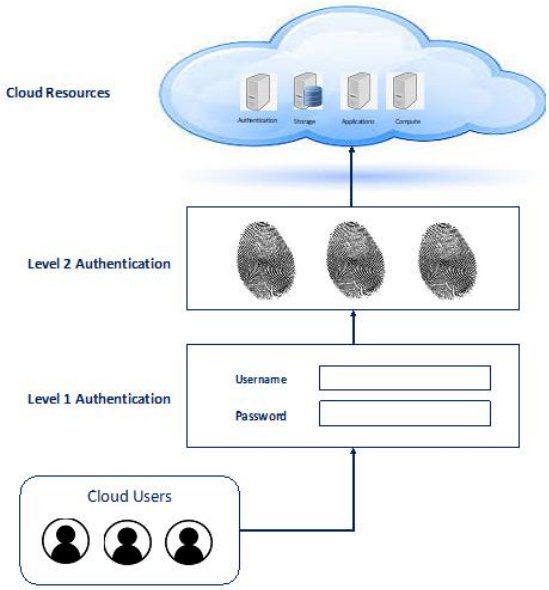


Figure 1 - Conceptual Design

3. METHODOLOGY

3.1 Type of Research

The type of research was a quantitative research. A system was developed, and data collected to analyze it.

3.2 Research Strategy

This research followed the design and creation strategy and involved designing, developing, implementing and testing an authentication system that incorporated username-password and fingerprint scan to control access to cloud storage resources

3.3 Techniques

Data Collection was done using documents and questionnaires. For sampling, the population in this research was selected through random stratified samples.

3.4 Data Analysis

Nominal data was collected through surveys, recorded and interpreted using mathematical formulas like mean, median and percentages. The results were presented in graphs, tables and pie charts.

Population Size: 37 respondents were selected from different demographic areas to participate in the pre and post implementation surveys that were carried out.

3.5 System Design and Development

The proposed system was designed using the waterfall model. This took a stepwise approach in designing, developing and testing the MFA system. Even though this model has limitations in real life situations where a clear view of all the requirements at the onset of the project may not be available, it was ok for this MFA system development as the requirements were clearly marked out right from the beginning and the laid-out steps were followed in the process.

The high-level system architecture and system components are portrayed in **figure 2** and **table 1** below respectively.

Table 1- System Components

Component	Description/Function
End User	Actual cloud user that is authenticated via login/password and fingerprint scan to access cloud storage.
Admin User	Super user that perfoms administrative activities like system implemntation and maintainance.
AWS Cloud	Amazon Web Services cloud that resides on the internet and is accessible via the public network. VPC is used to curb against security breaches like DDoS.
Virtual Private Cloud (VPC)	AWS networking layer that allows for definition of subnets within the virtual network.
Internet Gateway	Provides compute resources in the cloud that is easily scalable.
Elastic Load Balancer (ELB)	Acts a single point of contact for all client service requests towards the web application server running on EC2. The ELB that was used for this system was Application
Elastic Cloud Compute (EC2) Instance	Provides cloud computing resources like RAM, CPU, disks, networking interfaces etc.
Relation Database (RDS) Instance	This allows users to setup, a relational database in Amazon's cloud that allows ease of operations and scaling.
Simple Storage Service (S3)	Amazon's storage service that enables storage of data from anywhere over the web.
Public Subnet	The subnet that allows access from the internet
Private Subnet	A restricted subnet that is not accessible from the internet and facilitates communication between EC2 and RDS

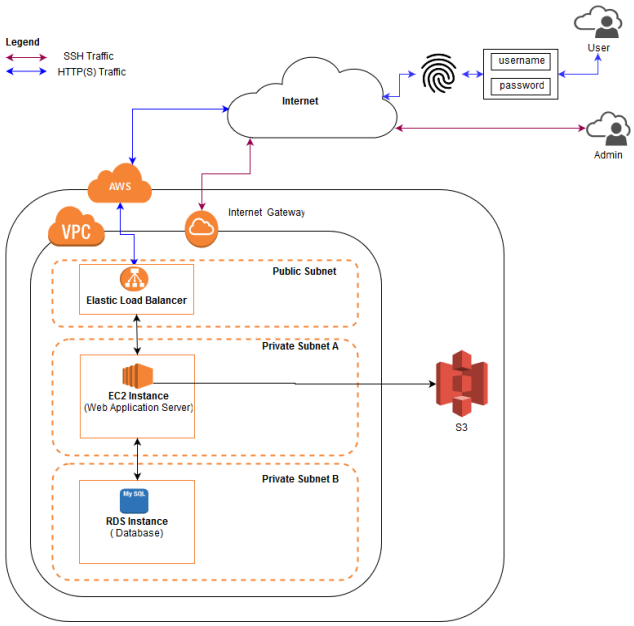


Figure 2 - High Level System Architecture

3.6 Algorithms

Two algorithms were used; ***fingerprint biometric enrollment that involved*** extraction of fingerprint templates, template matching, storage into the database (shown in **Figure 3**) and ***fingerprint matching*** where retrieval of the stored templates for comparison against scanned fingerprint was done (shown in **Figure 4**).

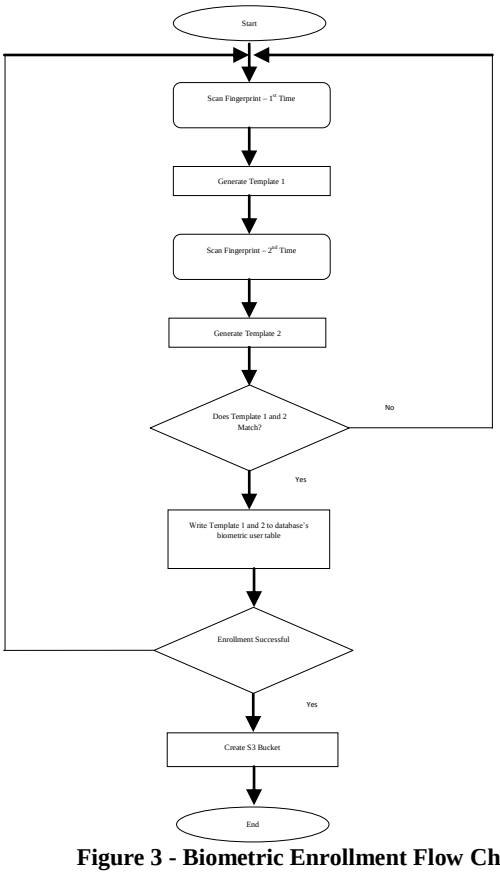
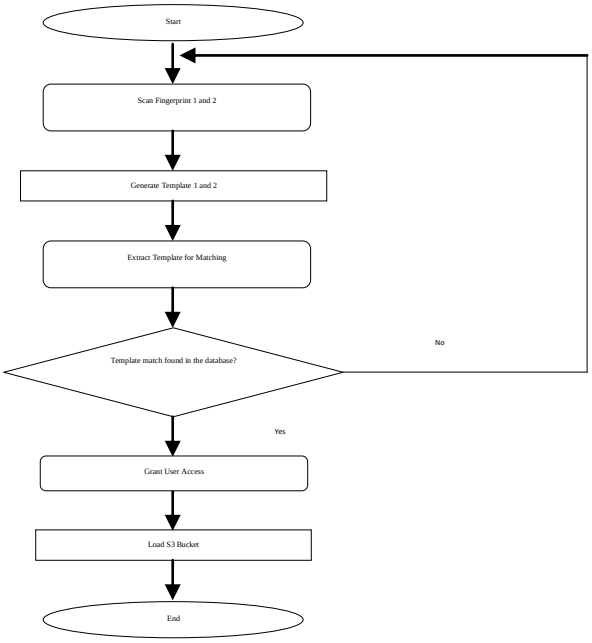


Figure 3 - Biometric Enrollment Flow Chart



3.7 System Modules

Registration Module

There were two steps of authentication involved and for each there had be registration taking place. The knowledge factors had to be registered and stored in the database first then biometric(fingerprint) data was scanned, the features extracted and stored in a template.

- **Username and password registration**

A user was required to enter credentials like first name, last name, user name, password, email address, security question and answer. The details were stored in MySQL database upon successful registration.

- **Fingerprint registration**

A was prompted from the registration page to scan his fingerprint from the connected hardware, details were extracted and placed in a template that was stored in the database.

Authentication Module

Once registration was successful for both authentication factors, the user was redirected to the login prompt where again two steps are involved.

- ***Step 1: Username and Password***
  The registered username and password were entered at the login page and there were checked against the data stored in the user database. If there was a match, access was granted, and user redirected to biometric login page.

- ***Step 2: Fingerprint scan***
  User was prompted to scan the enrolled fingerprint. The matching algorithm 1: N was applied to check the scanned fingerprint against the templates stored in the database and when a match was found, the user was successfully authenticated and redirected to the cloud storage interface.

Cloud Storage Module

Once the user is past the authentication stage, access was granted to their specific cloud storage bucket where they could list, upload, download or delete data/files. This ensured that they could only manipulate their own data but have no visibility to any other user's data ensuring data integrity, one of the metrics to be preserved in this paper

4. RESULTS AND DISCUSSION

This chapter presented the outcome of the research, data collection, system development and discussions on the same in relation to the problem that was being addressed in this paper. The researcher's contribution was presented in this section as well.

4.1 Results and Findings

4.1.1 Pre-Implementation Survey

Authentication Methods for Cloud Storage Users

In a bid to identify the current methods of authentication being used by cloud users to access data storage, questions were administered with options for the widely used authentication factors were floated. As in **figure 5**, about 99% of the sample set affirmed having a cloud storage account. As per the results shown in the figure below, almost all the respondents (approximately 97%) use the conventional knowledge factors for authentication as expected. In addition to that, other factors are in user so the assumption here is that with the hype on the use of multiple factors for authentication, usernames and passwords as well as one of the other factors like OTP, Phone Authenticator, Software Token and Fingerprint Scan. For the Fingerprint scan, unless the respondent has access to a private cloud that has employed the use of biometrics, the most popular free cloud storage service providers like Google Drive, Dropbox, pCloud and OneDrive use possession factors as a second authentication factor. It's also quite noticeable that other than fingerprint scans, other modes of authentication are not in use at all.

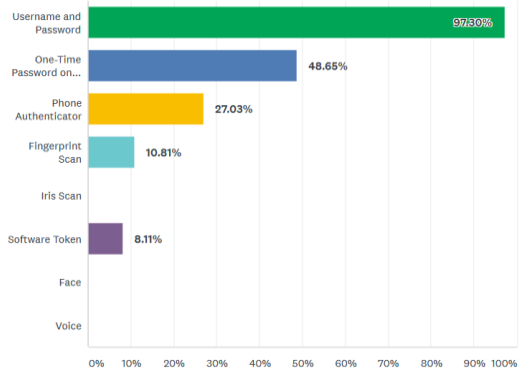


Figure 4 - Authentication Factors Currently in Use

Fingerprint Biometrics Preference over other biometric modes

Among the available modes of biometric authentication, fingerprint scan was a preference for approximately **60%** of the sample population. As indicated by a portion of the respondents, fingerprints are not invasive, and the scanners would not affect them. In comparison to iris recognition where rays from the biometric device would be used to scan the eyes, most users would refuse for fear of getting their eyes damaged. In addition to that, fingerprint scanning has been used over the years in various establishments such as medical insurance enrollment for SmartCare systems, it didn't come as a surprise that they would prefer this mode as compared to the others since they are already quite familiar.

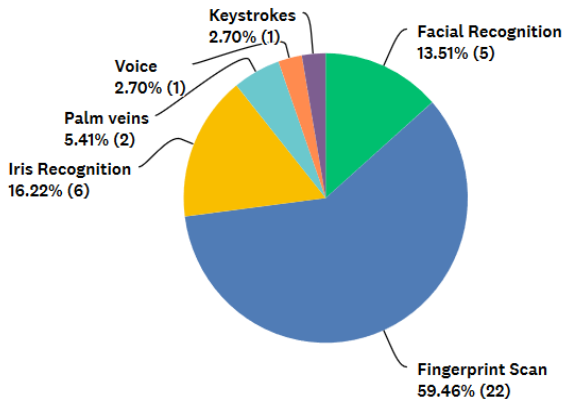


Figure 5 - Biometric Authentication Factors Distribution

Security Threats in the Cloud Computing Storage

Cloud computing became popular as time went by and the prevalence continues to grow with more people embracing cloud services. As the results in **Figure 7** shows, a good percentage of this sample size with cloud storage access, about 89 % considered security a threat to the data they store. This could have been due to the openness of cloud services with no proper control from the end users. About 11% of the people who filled the questionnaire however indicate that security is not a threat a threat from. This part of the sample population could have been drawn from those who do not understand the working of cloud computing or how open and pro ne to attacks it is.

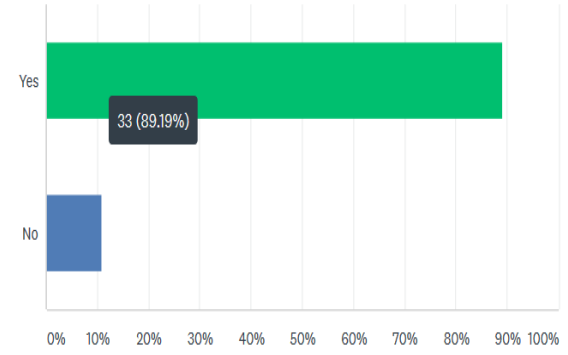


Figure 6 - Security as a Threat in Cloud Computing

4.1.2 Post Implementation Survey

A post-implementation survey was performed based to assess user perception and accuracy of the developed system. The respondents tested the system functionality after which a questionnaire was administered. In this section, a record of the outcome and results are discussed.

Usability

To determine the ease of use of the system, the researcher asked the respondents to rate their experience and 9 out of the 12 indicated that the system was very easy to use. For 1 respondent, the usability of the system was average whereas the other 1 indicated it to be good. Being a web-based system with straightforward steps to register and authenticate using username and password as well as fingerprint scanning, this can be applied by any cloud data storage users regardless of their technical background and capability as was seen during the assessment.

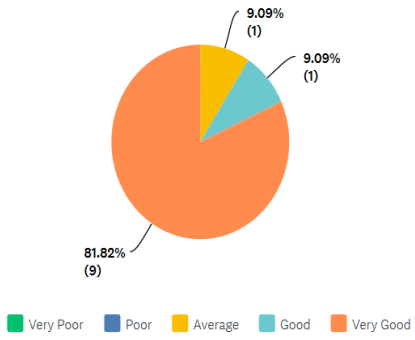


Figure 7 - System Usability

User Perception

As indicated in **Table 2**,11 out of the 12 respondents indicated that they would consider using such a system that incorporated biometrics on a day to day basis. The reasons that they gave for this are shown in the table below with most of them considering the added layer of security that biometrics brought to the authentication process thus ensuring security. Some also stated the ease of use and operation as a point that would make the use the system whereas for others it was the ability of the system to accurately identify them. 1 respondent didn't understand what authentication and security was hence didn't see the relevance of the system to them as he didn't have access to cloud services.

Table 2 - User Perception of the System

Respondent	Perception of the Developed system
1	Secure
2	It's very secure and its difficult for anyone with different fingerprint to log in
3	To prevent pseudo users to access one's account
4	Ease of use and fingerprint identification which adds extra security layer
5	Use of biometric ensures high security for a user account
6	It's easy to access and operate
7	Respondent would be assured of data security
8	Combines 2nd factor authentication with a human presence
9	It provides more accurate identification.
10	More Secure layer added onto of the conventional authentication
11	It's very easy to use
12	Does not use cloud storage services

4.2 Discussion

In a bid to understand why biometrics has not been incorporated in Cloud Data Storage, it was evident from the conducted survey and a review of previous studies that many attempts have been made at incorporating different forms of biometrics like multi-modal biometrics i.e. more than one mode with well formulated theories but still no clear adoption is evident from the currently available cloud service provider platforms.

The proposed system in this research sought to incorporate biometric fingerprint scans that would facilitate registration and authentication in the cloud and this implied all the authentication would be done over the web. This was achieved as detailed in Chapter 3: Methodology enabling users to enroll both their knowledge factors, as well as biometric data that was then stored in a secure database as templated and retrieved during the two-factor login. Tests were conducted on the developed system to ensure confidentiality and integrity were preserved with the second layer of authentication that was included in this project.

4.3 Contribution

In conducting this research, the aim is to address the challenges faced with access and authentication leaks to systems by incorporating MFA, specifically biometrics. Whereas the point of focus here has been on cloud computing storage, this can be applied in private clouds as well since several organizations are embracing and migration theory on premises system to the cloud. This would help them secure their data in such cloud environments by ensuring only authorized users access the same. In addition, many cases have come up on organizational data being compromised, swindling of funds in government ministries with the culprits claiming their knowledge factors were stolen as was the case of Integration Financial Management Information System (IFMIS). This system would come in handy to ensure that the top authorized personnel to handle such sensitive transactions or information get to enroll their biometrics for system authentication hence ensuring confidentiality and integrity of the intended data.\

5. CONCLUSION

5.1 Summary

This research was conducted to determine how biometrics can be incorporated in multifactor authentication (MFA) for cloud computing storage. Even though MFA is already in use with possession and knowledge factors, there are still security threats like brute force and dictionary attacks and loss of possession factors like tokens that hinder the adoption of cloud computing. Despite being more secure, none of the cloud service providers have incorporated biometrics in cloud data storage and this was found to be due to the challenges faced in availing biometric devices to the billions of users worldwide. Various multimodal biometric have been proposed in previous studies however these have not been practicalized yet hence the leaving room for further works. A biometric system was developed and evaluated in this research to address security challenges in cloud computing data storage. The system allowed authentication over the web. It was found that cloud storage users would very much like to use biometrics (fingerprint scan) in authentication for the same, however, these have not been made available yet.

5.2 Challenges

While conducting this research, one of the major challenges experienced was finding the right biometric device that would be programmed and integrated with the cloud hosted web application to access cloud storage services. Of the myriad models of biometric fingerprint scanning devices that were available in the market, finding one that had an API or SDK that would integrate to the web application was not easy. Eventually, SecuGen Hamster IV that had an SDK and Web API was used to develop this prototype. However, it only had the capability to work on a Windows based client and not any other operating system. These biometric devices were quite expensive and having each user access biometrics considering the numbers that are willing to embrace the same, it would imply that each of them has access to such a device which doesn't seem practical for cloud service providers that offer services over the public cloud to billions of users all over the world. This would explain why biometrics have not been adopted by the cloud computing giants like Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, Rackspace etc.

5.3 Future Work/Recommendations

Cloud evolution is a going concern with most public and private organizations/businesses migrating to the cloud hence security is very key. Incorporating inherence factors in multifactor authentication is one such way to ensure security threats and breaches are minimized. Whereas it was possible to build a protype that allows biometric authentication over the web, there is still working to be done to ensure interoperability of biometric devices with cloud applications. Enabling compatibility between biometric devices that are available in laptops, phones, and such applications to facilitate mass roll out is an area that some research can be done to enhance the adoption of biometric authentication in cloud computing.

6. ACKNOWLEDGMENTS

The authors wish to show appreciation to the University of Nairobi for creating a conducive environment to conduct this research and to all the respondents that agreed to answer questions and review the developed system.

7. REFERENCES

[1] Mosca, P., Zhang, Y., Xiao, Z., & Wang, Y. (2014). Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. Int. J. Communications, Network and System Sciences, 529-535.

[2] Amazon Web Services Inc. (2019, January). *Multi-Factor Authentication*. Retrieved from Amazon Web Services Inc.: https://aws.amazon.com/iam/details/mfa/

[3] Padma, P., & Srinivasan, S. (2016). A survey on biometric based authentication in cloud computing. *International Conference on Inventive Computation Technologies (ICICT)* (pp. 1-5).

[4] Soofi, A. A., Khan, M. I., & Fazal-e-Amin. (2014). A Review on Data Security in Cloud Computing. *International Journal of Computer Applications, 94*(5).

[5] Panse, D., & Haritha, P. (2014, August). Multi-factor Authentication in Cloud Computing for Data Storage Security. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(8).

[6] Soni, P., & Sahoo, M. (2015). Multi-factor Authentication Security Framework in Cloud. International Journal of Advanced Research in Computer Science and Software Engineering Computing, 5(1).

[7] Cloud Security Alliance. (2016). Cloud Security Alliance Releases 'The Treacherous Twelve' Cloud Computing Top Threats in 2016. Retrieved from Cloud Security Aliance: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

[8] Be'ery, T. (2015, 02 24). How Attackers Likely Bypassed Linode's Two-Factor Authentication to Hack PagerDuty. Retrieved 02 11, 2019, from Security Week: http://www.securityweek.com/how-attackers-likely-bypassed-linodes-two-factor-authentication-hack-pagerduty

[9] Veerendra, B., & Prasad, Y. (2017). A Trusted Framework for Authentication and Security for Business Applications in Cloud. International Journal for Modern Trends in Science and Technology, 03(01).

[10] Naveed, G., Rakhsh, & Batool, a. (2015). Biometric Authentication in Cloud Computing. Journal of biometrics & biostatistics, 6(5). Retrieved 3 11, 2019, from https://omicsonline.org/open-access/biometric-authentication-in-cloud-computing-2155-6180-1000258.pdf

[11] Qaddour, J. (2018). Multifactor Biometric Authentication for Cloud Computing. The Seventeenth International Conference on Networks.

[12] Choudhari, E., & Bodhe, K. D. (2017). Biometrics Authentication Technique in Cloud Computing. International Journal of Scientific Research in Education, 5(01). Retrieved 3 11, 2019, from http://ijsae.in/index.php/ijsae/article/view/65

[13] Sasi, E., & Saranyapriyadharshini, R. (2015, March). Secured Biometric Authentication in Cloud Sharing. International Journal of Computer Science and Mobile Computing, 04(03), 572–577.