Designing a Secure Higher Education Credentials Authentication Framework Using Cloud Computing Concept in Ethiopia

By: Adisalem Hadush

A Thesis Submitted to the

Department of Computing

School of Electrical Engineering and Computing

Presented in Partial Fulfillment for the Degree of Master of Science in Software Engineering

Office of Graduate Studies

Adama Science and Technology University

Adama, Ethiopia

July, 2019

Designing a Secure Higher Education Credentials Authentication Framework Using Cloud Computing Concept in Ethiopia

By: Adisalem Hadush

Name of Advisor: Dr. Ravindra Babu.B

A Thesis Submitted to the

Department of Computing

School of Electrical Engineering and Computing

Presented in Partial Fulfillment for the Degree of Master of Science in Software Engineering

Office of Graduate Studies

Adama Science and Technology University

Adama, Ethiopia

July, 2019

Declaration

I hereby declare that this MSc Thesis is my original work and has not been presented for a degree in any other university, and all sources of material used for this thesis have been duly acknowledged.

Name: _____

Signature: _____

This MSc Thesis has been submitted for examination with my approval as thesis advisor.

Name: _____

Signature: _____

Date of submission: _____

Approval of Board of Examiners

We, the undersigned, members of the Board of Examiners of the final open defense by _____ have read and evaluated his/her thesis entitled "_____" and examined the candidate. This is, therefore, to certify that the thesis has been accepted in partial fulfillment of the requirement of the Degree of ……

_____	_____	_____
Supervisor /Advisor	Signature	Date
_____	_____	_____
Chairperson	Signature	Date
_____	_____	_____
Internal Examiner	Signature	Date
_____	_____	_____
External Examiner	Signature	Date

Acknowledgement

First of all I would like to extend my deepest gratitude to the unpaid ever help of the Almighty God starting from the beginning to the completion of my research work. It is all His work to have the courage and persistency for achieving once dream. I have no words to thank Him enough for all His grace, guidance and unlimited pleasures and blessings.

Secondly, my special sincere thanks go to my advisor, Dr. Ravindra Babu.B for his patient and honest guidance and advice that enabled me to keep my strength and hope to finish this research work. His kindness and concern to provide all the possible helps he can offer to me was equipping me with motivation and determination to keep working hard towards the completion of my thesis work. I sincerely thank you him for all his kind and patient guidance and advice.

Last but not least, I thank my family- my wife (Lielti Hafte), my children (Edna & Euel) for their support, prayers, and encouragement through all the time of this thesis work. They were the source of responsibility and inspiration to realize my potential to achieve my dreams.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AJAX JS	Asynchronous Java Script and Extensible html
APIs	Application Programming Interfaces
ASP	Active Server Page
SHECAF	Secure Higher Education Credentials Framework
CCRA	Cloud Computing Reference Architecture
CMS	Credential Management System
CSS	Cascading Style Sheet
EA	Enterprise Architectures
EAF	Electronic Authentication Framework
E-Authentication	Electronic Authentication
E-government	Electronic Government
E-Services	Electronic Services
E-Verification	Electronic Verification
HEC	Higher Education Credential
HEI	Higher Education Institute
HEIs	Higher Education Institutes
HERQA	Higher Education Relevance and Quality Agency
HTML	Hyper Text Markup Language
HTTPS	Hyper Text Transfer Protocol
IaaS	IaaS- Infrastructure as a Service
IAM	Identity and Access Management

IBM	International Business Machine
IBM CCRAs	International Business Machine Cloud Computing Reference Architectures
ICT	Information Communication Technology
ICTs	Information Communication Technologies
IDE	Integrated Development Environment
IIS	Internet Information Service
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Token
MOE	Ministry of Education
MVC	Model View Controller
NET	Network Enabled Technology
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PKI	Public Key Infrastructure
RA	Reference Architecture
RF	Reference Framework
RM	Reference Model
SaaS	Software as a Service
SDK	Software Development Kit
SLA	Service Level Agreement

SMART	Specific Measurable Achievable Realistic Timely
SMS	Short Message Service
SQL	Structured Query Language
SSH	Secure Shell
SSO	Single Sign-On
UI	User Interface

Abstract

Hiring employees based on a set of selection parameters is a common practice all over the world. Education qualification and training credentials are the most widely used and essential requirement during recruitment of employees.

In Ethiopia, due to the need to hire educated manpower has increased, the number of higher education institutes and graduates have increased dynamically. However, a number of public services reported to have hired employees with a fake academic credentials. Prospective employer companies have been hiring unqualified employees. This leads to a big socio-economic failure. Therefore, there is need to ensure the validity of employees' credential across the country. However, there is no common platform for detecting the legitimacy of higher education credentials. The current authentication method has not any mechanism to detect fake credentials.

This research study conducted a detailed investigation on the current methods and challenges of authentication for higher education credentials, how a secure cloud based E-authentication can be designed, developed, and tested. Therefore, the aim of this research is to develop a secure E-authentication prototype on the cloud technology by using a digitally signed Quick Response (QR) code in order to help Higher Education Relevance and Quality Agency (HERQA) in the authentication of higher education (HE) credentials for the prospective employers in Ethiopia.

QR code scanning mobile and cloud web applications were developed to save time, effort and provide convenience for stakeholders that participate in the credentials authentication process. The study used questionnaire, Interview, and observation data collection techniques and the developed prototype and proposed framework were evaluated by different users and information technology (IT) professionals. The result of this research work was the design and development of a secure private cloud based framework and web application software as a service for higher education credentials (HECs) using mobile application. Moreover, majority of the respondents indicated very good (4) on the potential of the developed prototype to solve the integrity and security of HECs.

Finally, a systematic study on a more effective technologies for ensuring the integrity and security of higher education credentials and the development of fully automatic authentication method that supports both offline and online verification were recommended.

Keywords: **Authentication, HE credentials, cloud computing, QR code, digital signature**

Chapter One: Introduction

1.1 Background of the study

The expansion of higher education and massively increased number of graduates in the country has led employer companies to seek highly qualified employees [1]. Because of this employees who cannot attain the desired qualifications opted to use fake degrees to secure their job status [1]. Nowadays, a number of civil servants has been reported being employed using a forged higher education credentials by several local media news. As cited in [1] the local media Addis Zemen (20 October 2017) reported 7000 employees in the largest region of Ethiopia, disclosed themselves for using false credentials. Similarly, 40 employees from Gambela region and 500 employees from Amhara region confessed for breaking the law [1]. The production of forged credentials have been increased with advancement in technology and the availability of printing and editing tools at low cost [2 - 4]. In addition, the inability of the traditional security mechanisms to go in line with these modernity to detect the ingenuity of the credentials has its own contribution to the forgery practice. This enables unqualified individuals to work at critical working positions illegally. Succeeding in using fake higher education credentials leads to various failures at individual level and national level. For instance, according to [5] it can bring the following risks to employer organizations:

- ➔ Increased employee leaves
- ➔ Employee replacement costs
- ➔ Humiliation and damage of reputations
- ➔ Lack of trust from public
- ➔ Losses of customers and profits
- ➔ Damaged competition
- ➔ Facing to legal actions
- ➔ Increased Corruption
- ➔ Deteriorated public service
- ➔ National failure

Recently there is a move towards the improvement of quality education and reducing corruption by the government of Ethiopia. As a result, most organization has started to review documents of old employees and new employees seriously. This action has led to find several employees with fake documents by using self-revealing, cross checking with sources of the documents and informers. [1], [6 - 9]

As a consequence of the challenges of the current authentication technique of higher education techniques and the new move towards the improvement of quality of education and reducing corruption there is a need to use a better approach that is robust, fast, and reliable that can authenticate the originality of higher education credentials instantly and effectively.

As a result, this research study has proposed and developed a digital system based on a secure QR code containing a digital signature signed by a private key of the certificate authenticating body, in our case the higher education relevance and quality agency (HERQA). Furthermore, the researcher has conducted vast researches to select the digitalization approach in order to implement the new electronic system. Due to its convenience, cost effectiveness, fast response, collaboration and configurability the fifth generation technology, the cloud computing [3], [10] is found an appropriate to implement the digital authentication system which involves large data and multiple interacting components. This designed and developed cloud based higher education credentials authentication framework to solve the problem of integrity and security for information on educational credentials and the authentication of their sources effectively in a real time. This creates an easier and smart environment for employers, HERQA and genuine document holders to automatically authenticate higher education credentials without the need to contact responsible officers in person.

Nowadays, The IT sector, especially the cloud IT has dominantly controlled the operations of systems and government services. A myriad organizations has been moving their systems to the cloud aiming at saving people's time, efforts and providing convenience. Communication ways between government and citizens has been changed highly by the use of ICT [10]. As a result, the development of e-government automations is being enhanced through time. Currently, Web services and cloud computing are the most promising technologies for accessing and sharing information and resources everywhere. Cloud Computing has recently been used in almost every industry.

With the rapid growth of Internet users, the needs, and demands of citizens to complete their tasks with minimal time, many government agencies are offering e-government services through the internet [10]. Automated operations are easier and simpler for use than these which appears to be operated on paper based. Therefore, to define electronic authentication (E-authentication), it is a suit of digital communication systems that help employers collaborate with various academic certificate authentication bodies to validate the authenticity of the documents of employees in the country. This enables to effectively connect various degree certificate issuing higher education institutions with employers to protect the use of fake documents by employees. Moreover, it is cloud-based, delivering all of the resources, application software, processing power, data storage, backup facilities, and development tools as a set of services over the Internet, allowing employers, universities, and certificate holders to save files from any local workstations using a public network and access off-premise applications without the need to host them at the in-house environment, thereby providing access to save files from any computer with an internet connection [5].

Using web services and cloud computing technologies, the entire electronic authentication was stored in one place in the cloud and made available to authorized users from everywhere through extensive access to the network. The application can be provided and controlled by the ICT department of the Ethiopian quality assurance (QA) agency, HERQA, which saves costs, time, and increase the intelligent accessibility to degree certificates that are issued by various academic institutions.

1.2 Motivation

Based on our observations and local newspaper, and local Medias report, a myriad civil servants in Ethiopia has been working in various government institutions with a false credentials especially with a fake education certificates. This clearly shows that there is not a good method of authentications for protecting fraudulent documents in the country. Currently, local employer companies and document provider institutions have weak coordination with each other which involves a traditional and manual based communication for tackling fake documentation. This way of verifying the correctness of the credentials involves various levels of human interactions which is a tedious and time consuming process [2]. This problem can be solved by transforming the paper based verification processes to an automated operations which are easier and simpler for use. Therefore, motivational research is to examine and identify the existing manual verification of

documents in Ethiopia by using different methods and solving with an efficient electronic system. This solution includes the design of secure cloud based E-Authentication framework and the development of prototypes. The proposed system initiative aims to support the core processes in the verification to deliver best-in-class services, transparency, accessibility, affordability, interactivity, and convenience within public employers and education institutions.

1.3 Statement of the Problem

Nowadays, the number of Ethiopian universities and their capacity to accept students increasingly has grown. The growth rate of graduates as compared to the growth rate of job availability is higher as well. Previously, nothing more than a literacy education background was required to get a job offer. However, in the recent time, recruiting civil servants for work needs professionals with better qualifications and skills. This demand has led citizens to seek a short cut to get the expected minimum requirements for hiring. Therefore, public servants have been involving in perpetrating forgery for gaining illegal job benefits. Especially, the fraudulent of education certificates is widely practiced with in Ethiopia. [1]

For example, in Gambella regional state, nine high ranking employees were found using fake documents by manually verifying education certificates of 201 top state executives with cooperation of the Ethiopian ministry of education (MOE) [11]. Moreover, Tamrat [1], in reporting news written by local newspaper Addis Zemen (20 October 2017), tells that in the Oromia regional government state nearly 7000 employees reveal themselves for using fake documents based on the call for clemency by the regional government . Likewise, about 500 public servants from Amhara regional state and 40 employees from Gambella regional state have confessed for employing fraudulent credentials to maintain their earnings [1]. The fabrication of false credentials, or illegitimate degrees and diplomas is a worldwide issue [12] beyond Ethiopia.

Educational fraudulent and forged degrees have increasingly become a global concern since the last two decades due to the demand of high academic competency in hiring and the availability of sound quality desktop photocopying tools and online degree sales from the advancement in technologies and the growing in computer networks [12]. This shows the downside usage of ICT. However, it is obvious how ICT involves in solving complex day to day societal and government work operations and activities. In Ethiopia, both the federal and regional governments have not

still employed ICT to combat academic fraud while individuals and organized groups are using it effectively for producing forged documents to keep their earnings by selling it to prospective employees. For instance, various civil servants in Ethiopia were employed in many public institutions using false credentials [7]. This is the result of the traditional paper based means of certificate verification process.

In reality, manual document verification is very challenging for organizations to verify especially for the bulky collection of credentials that should pass through authentication. Easy and convenient methods are needed to verify the authenticity of hard copy official credentials since individuals are still succeeded in using false credentials bypassing the public notary organizations [7]. This is due to the reason printed documents have not comprehensive approaches that are potent for verification [7]. In this information technology age, business processing procedures, government office work operations and public service works have been transforming from manual based operations to an efficient and effective digitalized form of service delivery and task processing. Verification of education certificates and degrees is one of these government office works that needs the application of digitalization for combating the wide spread academic forgery.

As a result, this study identified several issues that should be alleviated with the proposed electronic solution. The major challenges for organizations to verify the validity of printed documents through the manual verification technique are that it is cumbersome, it is time consuming task, it is costly, it is susceptible to corruption, it is prone to damage or conceal of documents and it needs the interaction of multiple personnel. In addition, this technique of verification decreases the confidence of prospective employers towards the document provider organization as it is not adequate method to identify forgery. Similarly, this tarnishes the reputation of the higher learning institutions in the eyes of the public. In particular, professions that need high degree of caution like construction engineers and medical doctors can cause a potentially high harm to the nation. Furthermore, integration of all the legitimate potential employers, job applicants and education certificate issuer institutions requires high storage costs, highly skilled man powers. In addition, there is a weak cooperation between the different educational institutions across the country and Higher Education Relevance and Quality Agency (HERQA) which results in dissatisfied public employers and quality service seeker customers [1].

Therefore, to end these problems this study would focus with the development of secure cloud-based electronic authentication/verification framework and prototype implementation that provides an automatic verification of higher education credentials to employers and employees.

1.4 Research Questions

The following questions were to be addressed by this study:

1. What are the current methods and challenges for authentication of higher education credentials?
2. What are the current modern technologies adoption and implementation models for E-authentication of higher education credentials?
3. How can a cloud framework be designed, developed and tested to authenticate higher education credentials?
4. Does the proposed cloud framework and prototype for authentication of higher education credentials solve the challenges faced by the current techniques?

1.5 Purpose of the study

The use of forged Academic credentials has been a concerning issue for a long time in the potential employer sectors communities, academic communities, and in the public community as a whole. As a result, secure higher education credentials authentication framework (SHECAF) is proposed to address this issue by creating a smart environment, digital workplace, and collaborations for Ethiopian prospective employers and higher learning institutions to protect the authentic credentials and to confirm the identity of the issuing institutions. This will ultimately result in improvement of employers and applicants potential to deliver quality service, to avoid the weak multi personnel communication among employers and higher education institutions which are the potential academic credential providers by developing and implementing an automated web based education verification system in a secure cloud computing environment, by utilizing digital signature and hash values with in a QR code.

The design also used to create opportunities for the competitiveness and improvement of the quality of education in the country. In addition, the proposed system allows implementing cloud-based E-authentication system in Ethiopia, collaboration and adding cloud-computing features and

architecture in the area of electronic authentication. Furthermore, to improve the verification and authentication processes and to evaluate a cloud-based architecture by ICT professionals and other experts in software engineering and related fields.

1.6 Objectives

1.6.1 General Objective

The main objective of this research study is to design and develop a secure cloud framework and prototype of an E-Authentication of higher education credentials in Ethiopia on the basis of QR code and digital signature technologies.

1.6.2 Specific Objective

The specific objectives of the study are the following:

- To investigate the challenges and current techniques to verify higher education credentials
- To conduct an intensive literature review on cloud-based E-Authentication of higher education credentials and E-governance.
- To collect and prepare appropriate data from different sources to design a framework and develop a prototype implementation.
- To identify the best cloud computing platform and to conduct survey of potential use of cloud computing technologies for the authentication of higher education credentials.
- To design, develop and test a cloud framework and prototype for E-Authentication of higher education credentials
- To evaluate that the cloud framework and prototype for E-Authentication of higher education credentials solves the problems faced in the current verification techniques.

1.7 Scope and Limitations of the Study

The main purpose of the study is to design a secured cloud-based electronic authentication of higher education credentials in Ethiopia. For the developed prototype, a framework was developed, which was deployed on a private cloud platform and would not have a complete implementation; because it needs more time, budget, and service level agreement from the cloud service provider. The population of the study is composed of HERQA higher education (HE) permit, accreditation and credentials authentication issuance experts. The framework can accommodate the integration of several universities to provide the electronic verification of their education credentials or certificates through a self-describing web service JSON. This technology is one of the reason for

the existence of the service oriented architecture feature in the cloud computing. Therefore, the framework can be used and accessible by all institutions either the issuing institutions or employers in common. The study was limited to higher education relevance and quality agency for data collection.

1.8 Significance of the Application

The result of this research will contribute to the ongoing research in this domain area. It will be an input for different researchers, software developers, and students. The main beneficiaries of the results will be the potential employers, job applicants, employer agencies, the academic institution community, and the public community as a whole. Likewise, it provides its own contribution to the beneficiaries such as government, university, developers, researchers, customers, and employers, employees across the country by digitizing the tedious academic certificate authentication or verification process and it is routing, using different technologies like cloud providers on accepting cloud computing services. In addition, this study is significant because it adds both theoretical and practical knowledge and believes to bridge the gap of research work.

Employers, applicants, higher learning institutions and the citizens as a whole benefits from the usage of the proposed E-authentication.

Benefits for employers**:**

- Enables mobilization of electronic authentication application. The employers in Ethiopia will access the application of electronic authentication anytime anywhere using their mobile phone, PDAs, PCs and other electronic devices.
- Used to create smart environment and digital workplace solution in which the employers should have good knowledge in technology and increase employee satisfaction.
- Encourage innovation by releasing time from unproductive processes and employee energy.
- This study mainly used by developers by understanding the proposed framework and prototype-developed system to implement the full system.
- Save time and money either on exchange of applicant education credentials by email/mail or on going down to issuing institutions for authentication
- Make the hiring process easier because nobody have to compare the credentials
- Make hiring decisions based on verified information

Benefits for certificate issuing institutions:

- Plays a vital role in maintaining the reputation of the institution by protecting fraud certificates using the name of the institution
- Increases the credibility of the institutions in the eyes of the public and the employer organizations

Benefits for applicants:

- Save time and money for the legitimate applicants by avoiding the direct trip to institutions for authentication
- Obtain access to verified credentials immediately up on authentication
- Make application process easier because there is no need to contact multiple personnel in pursue of authentication

Benefits for the citizens:

- Improve the civil and criminal liability of fraud perpetrating
- Increase the quality of applications thereby leading to competitive applicants
- Creates a better quality of service and satisfaction of public service customers by blocking illegal employment

1.9 Organization of the Thesis

This thesis work is organized in eight chapters. As we have discussed in this section, the first chapter presents introduction. The rest of this work organized as follows: Chapter 2 presents a review of literatures and related work on a secured cloud-based E-authentication, E-governance frameworks; and the details of various related works that related to our work. Methodology of the work presented in Chapter 3.The design of the proposed framework discussed in Chapter 4. Chapter 5 presents the development of the prototype. Chapter 6 presents the evaluation, discussion, and result. Finally, in chapter 7, conclusion remarks and future work discussed.

Chapter Two: Literature Review and Related Works

2.5 Introduction

This chapter provides research background information from different sources such as books, peer reviewed journals, international conference papers and articles that are related to the objective and method of the present study. In addition, it helps to identify best practice and analyze the current status of knowledge in the area of the research. First, it provides understanding forgery of paper documents, forgery preventing technologies, overview of electronic authentication, the need, and benefits of electronic certificate authentication. Secondly, it explains about cloud computing; cloud computing service delivery and deployment models; cloud computing reference architecture, model, and framework. Lastly, works done by other researchers in the area that related to our study are discussed.

2.1 Forgery of paper documents

Falsification of paper based documents has a long history of concern in various organizations be both private and public. The development of inexpensive modern printing, scanning and editing tools has a big impact to the proliferation of producing an exact copy of documents that have indistinguishable resemblance with the genuine one [2], [5]. In addition, the inability of the traditional security mechanisms to go in line with these modernity to detect the ingenuity of the documents has its own contribution to the forgery practice. As a result of this, several organizations have been failed to identify the true information on official documents [13]. Consequently, these organizations has been long suffering from income declination and loss of reputation. This is because of the lack of a reliable and robust technique that enables to ensure safety and consistency of the data on the paper based documents [5].

There are different types of documents that are prone to the act of forgery. However, this study focuses on the higher education credentials that are issued by myriad private and public universities and colleges throughout the country.

2.2 Employee hiring concerns

Forgery is a growing practice in the employment environment. Employer organizations review educational credentials of job applicants to determine if the applicant is a qualified candidate for

their institutions. In addition to this, they consider the validity of the sources of the qualifications to the candidate. However, all recruiters and employer organizations in Ethiopia lack an adequate technique to determine if the applicants' documents are valid and/or how to handle cases where there is a suspicion of fraud. This requires a new concept that can provide the ability to detect and report such cases.

2.3 Types of document forgery

Counterfeited documents are classified into five different categories [14], [15]. These are:

- **Fabricated documents:** documents from sources that are not available in reality.
- **Altered documents:** misrepresenting any part of data on the document.
- **Manufactured in house**: an illegal document created by a personnel of the institution.
- **Diploma mills:** producing false academic qualifications as if it was from an accredited institutions.
- **Interpretive translations:** misleading translations of original documents.

2.4 Technologies for preventing paper document security attacks

2.4.1 Cloud Service

Design and development of a document verification and authentication model and storing it on a cloud storage where it can be delivered as service, software as a service over the internet reduces the threat of attack to paper documents [3], [5], [16]. Software as a service can be accessed by web tools such as web browsers or other web application program interface (API). The cloud computing technology provides an authentication and authorization plug-in model that enables to keep installed applications safe on the cloud [5], [16]. This is because of users of cloud services can be assigned a personal authentication and authorization security interfaces by the cloud security service framework which enables access of information only for authorized entities to the cloud hosted applications [5]. More importantly, cloud service uses public key infrastructure (PKI) that makes use of digital signatures to securely exchange of information between two organizations, preventing illegal modification, edits, or transfers of sensitive data to untended third parties [5].

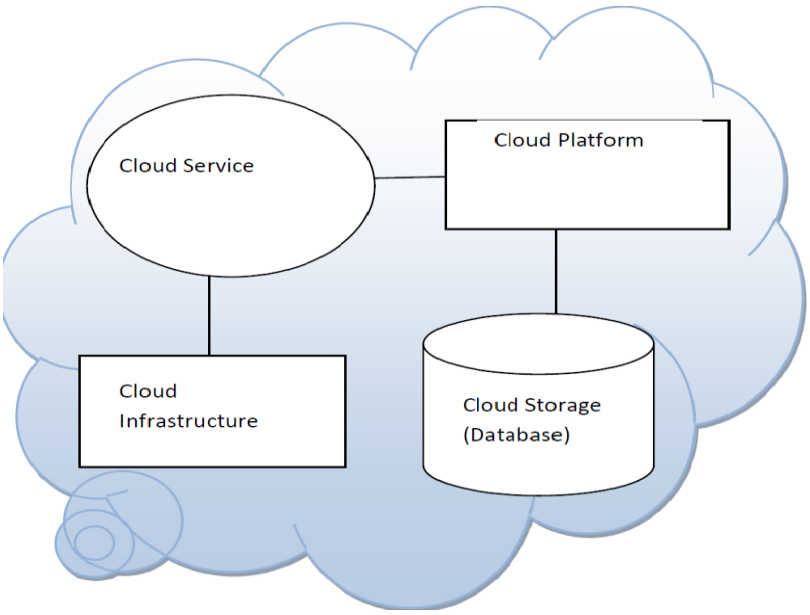


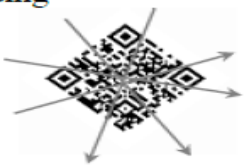
Figure 2. 1: Architectural Design in Cloud [16]

2.4.2 Quick Response (QR) code

QR code is one of the matrix barcodes, which the Japanese Denso Wave Corporation invented for an automotive industry [17]. The main purpose of the QR code is to store considerably large size of information related to the object it is printed on. Any type of information can be embedded into the two dimensional barcode, QR code. The information that QR embeds within is a code that can be read by mobile applications or other special readers that have cameras. QR code has been a research area regarding with its convenience for authentication and verification. Accordingly, many researchers have investigated that QR code is a preferable, popular, cost effective and fast technology that is widely employed in the area of document verification and authentication [2], [4]. Features such as large data storing capacity, error correction capability, reduced size print, high speed reading and flexibility and the proliferation of smartphones in the markets are the reasons for its popularity [17].

QR code has not any feature to protect the security of the data to be stored with in it. However, it is possible to use any encryption technology to secure it before embedding it into QR code [2], [4]

Table 2. 1: Features of QR codes compared to barcodes [17]

Feature of QR	QR code	Barcode
High capacity	Upto 7089 numeric digits 	10-20 digits 
Durability against soil and damage	Reading is possible (upto 30% damaged) 	Reading is impossible 
Reduced space	40 digits Numeric (approx 5 mm × 5 mm) 	10 digits numeric (approx.50 mm × 20 mm) 
360° reading	Supports 360° reading 	Horizontal reading 
Language supported	Numeric, Alphanumeric, Kanji, Kana 	Numeric, Alphanumeric 

2.4.3 Digital Signatures

Digital signature can be used at different levels of the ICT ecosystem. For instance, it can be implemented at the network, application, and database scopes. Digital signatures are implemented by using internationally accepted standards and algorithms such as hash function and public key encryption cryptosystems. They are a widely used technologies to provide authentication, security and integrity of information [2]. Therefore, digital signatures are very important to tackle and identify forgery.

Paper documents need the prevention from the threat of attack using digital signatures. Digital signatures can be printed on the paper documents being encoded with in a machine readable QR

code. Therefore, any individual organization who needs to authenticate the correctness of the documents can scan the embedded QR code using any QR code reader application installed on smart phones. This can solve the problem of manual verification which is insecure and involves non important steps that requires much effort and time to verify the documents. [2], [4], [13]

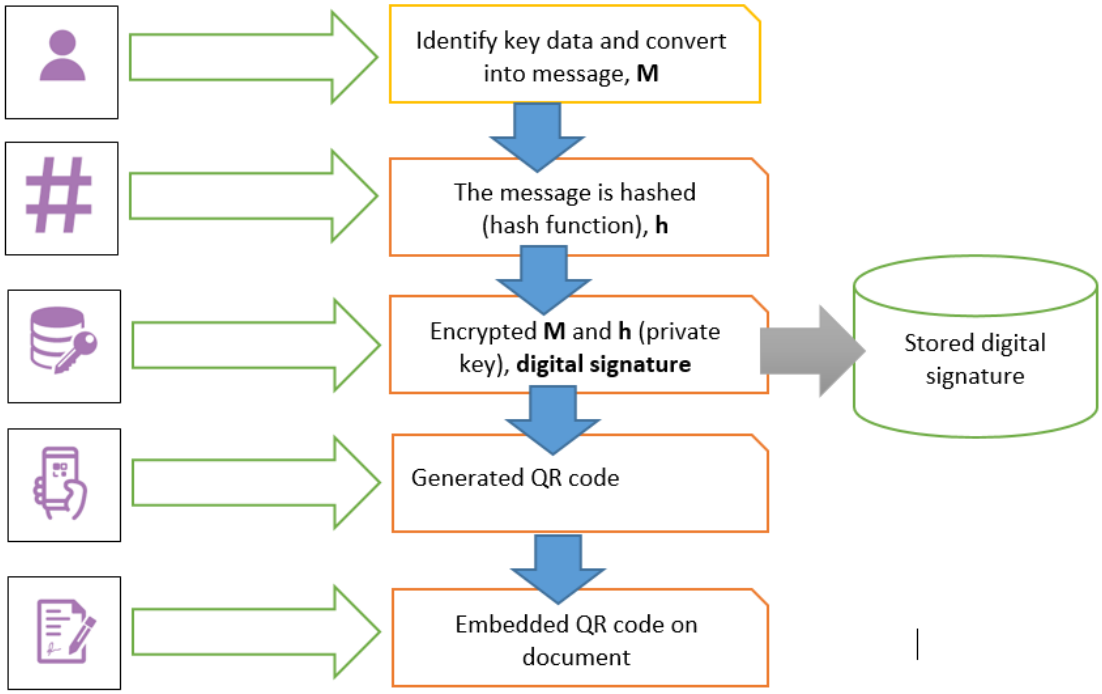


Figure 2. 2: Secure Document generation process

2.5 Overview of Electronic Authentication of Higher Education Credentials

Today, technologies are being developed and everything works with ICTs and employer and official document issuing institutions need to adapt to these ever-changing technologies and their problem-solving skills to protect forgery practices towards applicant's documents. Therefore, they need to build and develop their self-confidence in order to take advantage of the latest technologies, have the professional skills necessary to provide high quality authentication processes, manage the infrastructure to provide certificate authentication and make quick decisions.

In general, certificate authentication automation and workflow management, capture, storage, and control software are an electronic means of describing broad content and can assist in controlling content in conjunction with institutional processes and regulatory compliance [16]. It also aims to create a positive environment by eliminating the tedious number of documents and paper files,

streamlining desktop workflow by shortening processing time for authentication processes, and then focusing on the management system. It also allows the hiring companies and certificate issuing universities to improve the processing and transform paper-based official documents into a cloud-based electronic system. In addition, the design of most repetitive operations in the dynamic environment, manage the institutional knowledgebase; Increase the communication culture through collaboration and messaging.

2.5 Need and Benefits of Electronic Authentication

Nowadays, the responsibility for verifying certificate information is the responsibility of the officials of the organization. Given the large amount of information that passes through the various political, administrative, legislative and governance functions to verify credential documents is a cumbersome, costly and slow process that makes it impossible to track and manage the control of the information manually. It would be extremely useful to use an integrated system of collection, dissemination, and use of all these elements of action and information with control information. The efficiency, productivity, and control that can be exercised in the implementation of any decision can be increased by using such a system. Benefits include improved efficiency and reduced response time, consistency, tracking and control of fraud, reduced duplication, increased workflow control, better tracking, monitoring, and person independency [2].

2.6 Cloud Computing

In recent years, many IT professionals, business managers and researchers have begun to talk about a new phenomenon such as cloud computing. When invented is one of the first questions asked with the introduction of a new technology. In that, cloud computing has evolved through a series of phases that include grid and utility computing, provision of application services (ASP) and software as a service (SaaS). Each of these groups defined cloud computing differently according to their understanding of their offers.

“Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”[18].

The most recent and accepted standardized definition of cloud computing is the one by the National Institute of Standards and Technology (NIST) [19], [20]. The definition of NIST is concise, precise

and differentiates between enabling characteristics and technologies (i.e., virtualization) and between main and derived characteristics (rapid elasticity versus massive scalability); However, the definition ignores the business model of cloud computing, which is the main driving force behind migration to the cloud. The NIST definition is relatively technical and covers all cloud delivery models (public, private, hybrid and community) and, services model (IaaS, PaaS and SaaS) as shown in Figure 2.3.

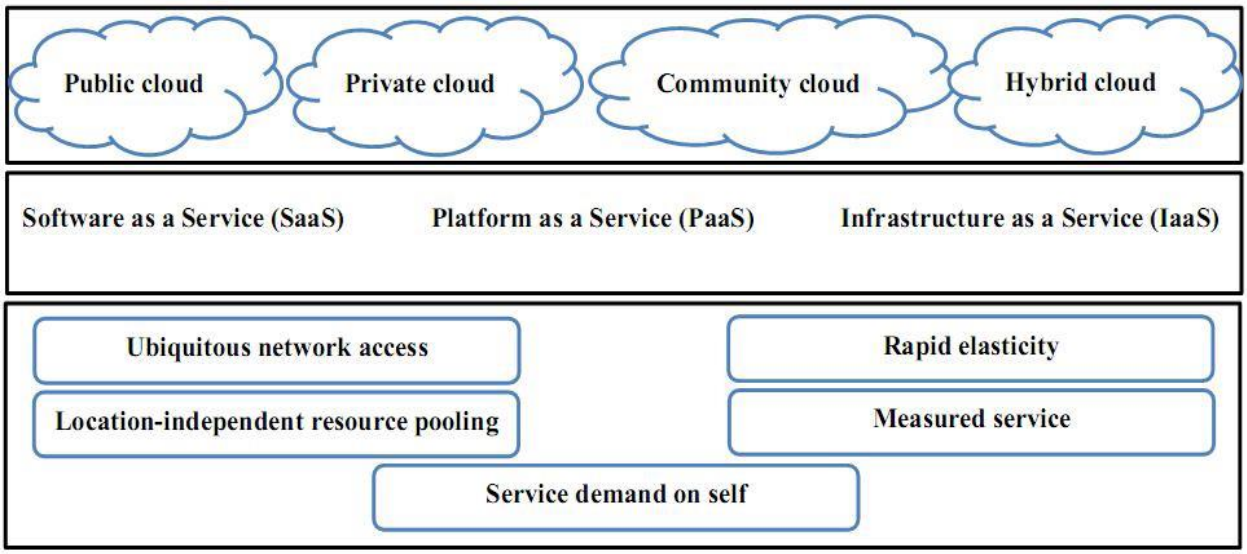


Figure 2. 3: NIST reference architecture [19]

2.6.1 Cloud Computing Service Model

Cloud computing uses the IT infrastructure as a service, and this service can vary from the rental of raw hardware to the use of third-party APIs. Cloud service models allow financial institutions to move from a capital-intensive approach to a more flexible business model that reduces operating costs. In practice, cloud service providers tend to offer services that can be classified into three categories: SaaS, PaaS and IaaS.

2.6.1.1 SaaS (Software as a Service)

In essence, SaaS is often used as a model where an application runs directly in the cloud and the user accesses it through the Internet. It refers to on-demand software, which is built on top of cloud's PaaS. As a result, Software that is implemented over the Internet with SaaS, a provider of an application's licenses to customers either as an on-demand service, through a subscription, on a "pay-per-use" model or (every time) no charge when there is the opportunity to generate income

from transmissions other than the user, such as ads or sales of user lists [21]. Customer has no control over the underlying infrastructure or platform, except application parameters for specific user settings [19]. “SaaS, is a software delivery method that provides access to software and its functions remotely as a Web-based service” [22].

2.6.1.2 PaaS (Platform as a Service)

PaaS defined as a computing service provider platform that allows the creation and deployment of web based applications quickly, easily provides virtual environments for and developing, deploying, monitoring, and managing applications online without and with the cost of buying and managing the corresponding software tools or hardware [22]. In the case of PaaS, the cloud provider not only provides the hardware, but they also provide a toolkit and a number of supported programming languages (such as .NET, java or python) to build higher-level services [19].

2.6.1.3 IaaS (Infrastructure as a Service)

IaaS is the capability provided to the customer different raw like storage space, computing, or network resources, operating system, applications, or any software that they choose. In addition, customer can manage the software deployed but not able to control the distribution of the software to a specific hardware platform or change parameters of the underlying infrastructure [19].

2.6.2 Cloud Computing Deployment Models

The different infrastructure deployment models differ in their architecture, the location of the data center where the cloud is deployed and the requirements of the cloud provider's customers (for example, due to regulatory, legal or other requirements). Therefore, clouds categorized based upon the underlying infrastructure deployment model as Public, Private, Community, and Hybrid clouds.

2.6.2.1 Public clouds

A public cloud is one in which the cloud infrastructure and computing resources are made available to the public over a public network and owned by an organization selling cloud services, and assists a diverse pool of clients [23]. A cloud service provider owns a public cloud’s physical infrastructure. Such a cloud runs applications from different customers who pay for their resource utilization on a utility computing basis, share this infrastructure, most often hosted away from

customer premises, and they provide a way to reduce customer risk, even temporary extension to enterprise infrastructure, and cost by providing a flexible.

2.6.2.2 Private clouds

A private cloud managed by the organization that consumes the services or a third party, and gives a single cloud consumer's organization the exclusive access to computational resources and usage of the infrastructure. Moreover, the cloud may be outsourced to a hosting company (i.e. outsourced private clouds), or hosted on the organization's premises (i.e. on-site private clouds) [23]. Private clouds offer highest level of security and privacy (not available to general public), improved reliability, performance and flexibility, and have total control but are expensive and need additional skill. Private cloud used to manage the secure data by the HERQA rather than third-party Cloud services provider.

2.6.2.3 Community clouds

Community cloud is the cloud whose infrastructure shared by several organizations and supports a specific community that has shared concerns and may be managed by organizations collectively or by a third-party Cloud services provider [24]. Community cloud used with cost effective, good security comparatively than the public cloud and shared among organizations.

2.6.2.4 Hybrid clouds

A hybrid cloud consists of two or more clouds, like on-site private, on-site community, off-site private, off-site community, or public clouds that remain as independent entities, but are interconnected by standardized or patented technologies to allow the transfer of data and applications [23]. While public clouds allow companies to outsource parts of their infrastructure to cloud service providers, they lose control over resources and the distribution / management of codes and data. In some cases, this is not desired by the respective company.

2.6.3 Cloud Computing for Authentication of Higher Education Credentials

It is providing the E-Authentication software as a service. The E-Authentication cloud model allows easy creation setup for academic certificates by selecting modules or subsets of E-authentication product suite according to their need. The model makes E-authentication deployment aims for easier and faster process for academic institutions and prospective employers

to start using e-authentication services. In addition, it integrates the Microsoft Azure service provider platform cloud services with electronic authentication services.

2.6.4 The Definition of Cloud Reference Model, Architecture, and Framework

In software engineering, a reference model (RM) is conceptual, abstract, technology independent framework, which represents the relationships between them and a set of domain concepts. It is usually used by domain experts who are working independently toward a standard [20]. When reference model concepts are arranged in a specific order (pattern) to provide a specific solution for recurrent problem, the generated architecture called a reference architecture (RA) [25]. While it is important to use the correct terminology when describing architectures, models, and frameworks, formality absent from several works that have been recently published in the domain of Cloud Computing. Together, the set of RMs and RAs create a reference framework (RF) [26]. For example, both NIST Cloud Computing Reference Architectures and IBM are more reference frameworks than reference architectures.

2.6.5 Comparison between Cloud Computing Reference Frameworks

As discussed in the previous subsection, various reference models, frameworks and architectures for cloud computing are being developed or are in development. The question is how to choose the framework or model, how these frameworks differ, and best suits our needs. The most obvious distinction between current reference frameworks, and models is that some of them are generic, while others are focused on specific areas. NIST has recently compared five specific architectures and six generic reference architectures in cloud computing [26]. The analysis of the current framework of reference shows that these frameworks were first, decomposed into architectural styles and principles, which are a set of rules and guidelines that guarantee that best practices are applied methodically; and, secondly, reference models consisting of architectural elements and their relationships.

There are many similarities between IBM CCRAs and NIST [26]. Figures 2.4 and 2.5 show the IBM Cloud Computing Reference Architecture and the NIST Cloud Computing Reference Architecture, respectively. We have used both of the cloud architecture ideas and concepts to design the proposed framework especially the relationship of cloud service model with electronic Authentication. While some architectural components are the same, both NIST and IBM CCRAs are comprehensive frameworks, and others have different wordings or are implicitly contained within other architectural components.

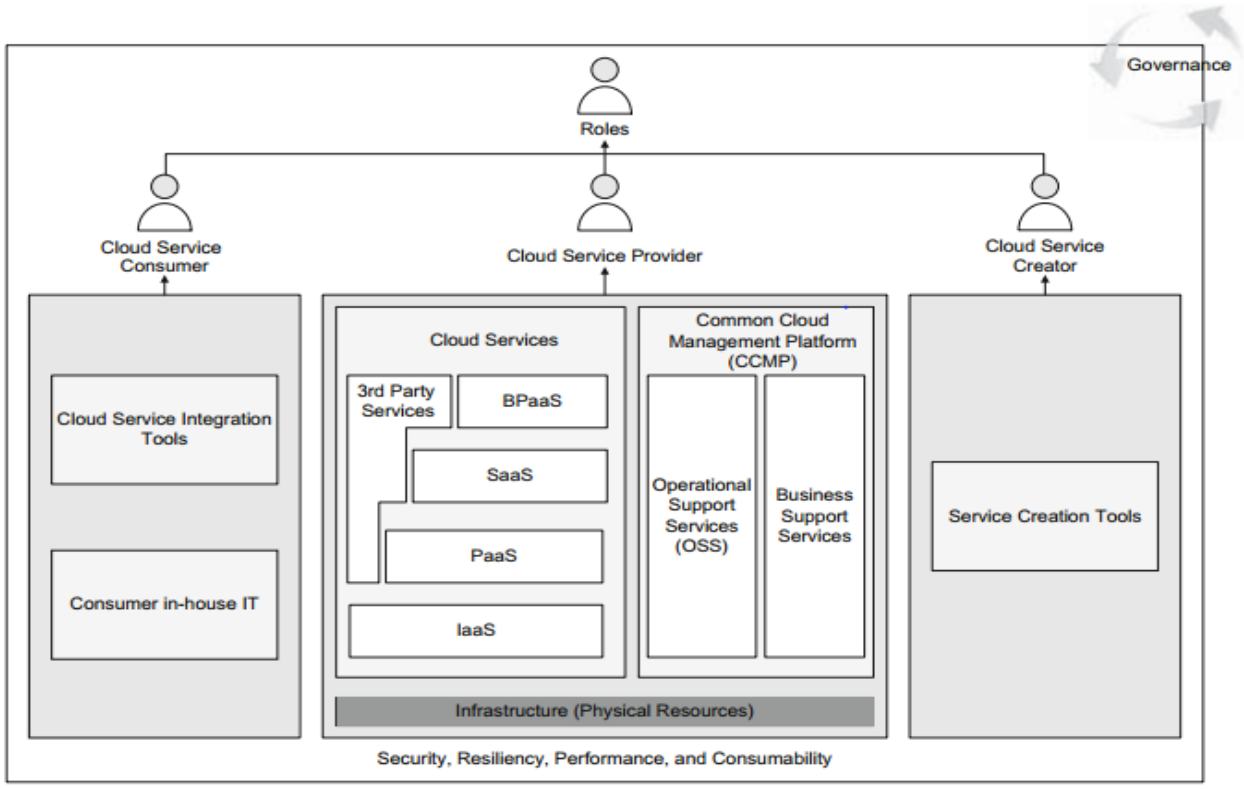


Figure 2. 4: An overview of the IBM Cloud Computing Reference Architecture [26], [27]

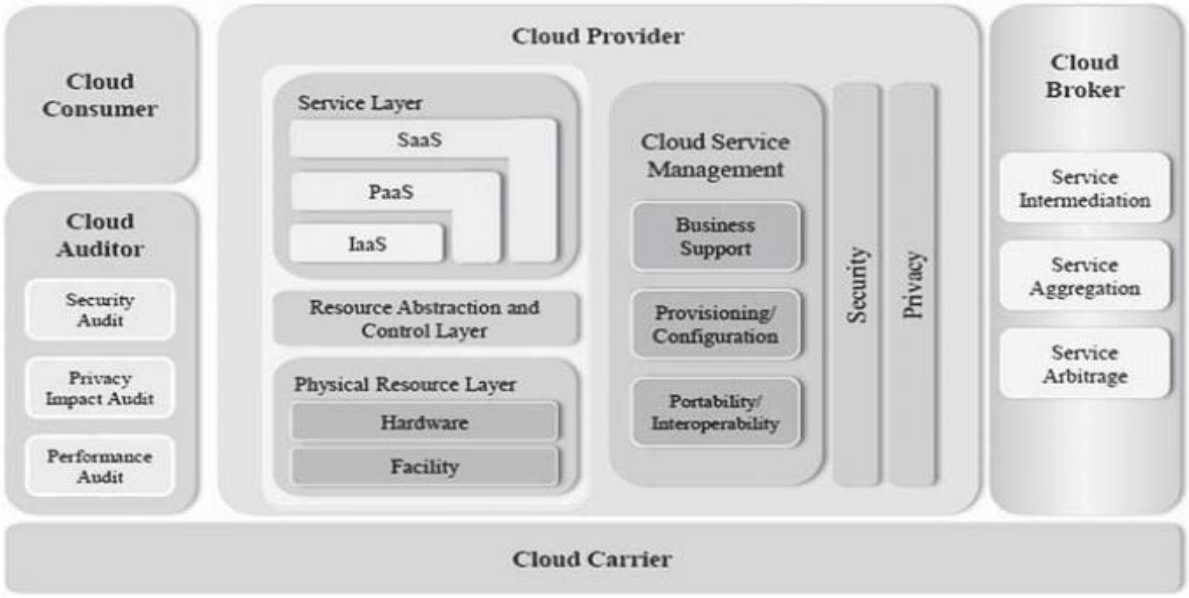


Figure 2. 5: NIST Cloud Computing Reference Architecture overview [23], [26]

2.6.6 Benefits of Cloud Computing

Cloud computing system is a robust and dynamic technology that has been increasingly growing in the IT industry due to the advancement in grid computing, distributed computing, parallel computing, virtualization and service oriented architecture. Cloud enables a measured, automated and adaptive service [18], [21]. HERQA needs innovative and cost effective methods to assist employers find more effective and efficient ways to root out the growing number of using fake higher education credentials. Electronic authentication on the basis of cloud computing and secure QR code technologies addresses the problem of traditional paper based authentication of higher education credentials. Cloud technology is the best alternative to manage and authenticate the large volume of educational credentials of job seeking individuals and employees across the country. We selected the cloud IT industry based on various criteria that the cloud framework can bring benefits to HERQA, Employers and both new and old employees. Table 2.2 shows the comparison of cloud with traditional IT.

Table 2. 2: Comparison of cloud with Traditional IT [5], [19], [26]

Criteria	**Cloud**	**Traditional IT**
Management efforts	Highly automated tools of management. Reduced costs	High manual monitoring and management efforts. High cost
Costs	- Cost based on usage and all resources and supports are provided by the provider - No upfront costs - Low risk of purchase - No version updates fight	- Dedicated infrastructure. Highest cos - Cost of resources(IT experts, hardware, network, software, support training) - High risk of purchase - Updating costs
Resource utilization	Effective usage of resources	High wastage of resources or over usage of resources
Availability	- Highly available 99.9% - Accessible anywhere and any time	- Higher downtime

Elasticity	Capacity can be increased and decreased easily	Difficult to scale up or down system capacity
Scalability	automatic handling for an increase in workload without noticing the difference	Challenging to manage and resize hardware resources to accommodate an increase in workload
Resources	No need of own IT experts and infrastructures	In-house IT experts and infrastructures are required
Agility	More Fast deployment and development, reusability, collaborative Fast start up. No installation and customization phase	Less agile
Security	Technical data security is high due to the available of highly professional experts	Less technical data security professionals

The comparison (table 2.2) shows that the cloud framework is more scalable, flexible, adaptable, reliable and cost effective than the traditional workstation. The cloud framework enables on demand scaling, measured service and on demand data storage resizing capability. Cloud computing provides the latest updated resources and services in less time. No need of updating and upgrading costs. Specially, for systems that are consist of a large volume of data and that growths continuously the cloud technology is the best and appropriate option to bring solutions. Authentication of higher education credentials involves a large number of parties that participate in the process of authentication. This needs an innovative, collaborative and cost effective method that solves such government services. The comparison in table 2.2 proves that the cloud environment is suitable for implementing our proposed E-authentication application. This is the reason we selected the cloud technology to transform the manual authentication technique to a digitalized, paperless and automated system that enables to detect fraud credentials effectively during recruitment process.

2.6.7 Limitations of Cloud Computing

Even though cloud computing brings money benefits regarding in cost reduction, quick development, scalability, efficiency, reliability, data storage management, power management and collaborative capability there are some concerns of privacy and security [5]. Most of the time data on the cloud is out of the control of the owner of the data this has been a significant concern about the security of the data despite the cloud providers has been done an intensive effort toward creating a safe environment [24]. Another limitation is that cloud computing is a connection based technology where it is impossible to access data on the cloud during offline [5]. The internet is always required to use the resources on the cloud environment.

2.7 Related Works

Many researchers around the world are exploring the possibilities of cloud computing, formulating new models, architectures, and cloud-based frameworks that help drive information and communication technology to implement different solutions in different sectors, such as Education, Finance, Healthcare, etc. In recent years, there have been many publications on various applications based on cloud computing. However, this section discusses some work on architecture and cloud-computing systems related to e-governance and e-authentication, in particular the framework for communication between government and citizens, institutions, businesses, co-operation and employers, and others Government authorities. Understand the need and benefit of cloud computing technologies in electronic authentication.

A.C et al. [16], the study Designed and developed a cloud based model that provide on demand access to certificates of several government sectors for both the users that request certificates and special privileged administrators that verifies, or rejects or signs the data for the requested certificate online. This model provides a convenient, on demand network access for a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts. Furthermore, the authors developed both private and public cloud models. The public cloud where a main remote server and the electronic application are placed, enables users to request and get certificates such as residential, income tax and land records etc. by filling application forms and attaching appropriate proofs such as voter id, driver license and ration card etc. online using any web tools. Whereas the private cloud provides access to data in the public

cloud by special privileged administrators to authorize certificates using digital signatures. The authors ensured data security and integrity by using RSVP security algorithm and ascertained effective search of the application in public and private using Cloudle cloud search engine.

In general the authors defined five stages to authorize certificates as shown below:

Stage 1: User requests the public cloud by filling application forms to get certificates online.
Stage 2: The uploaded user document is available on the cloud server and document progress notification is sent to users.
Stage 3: The verifier accesses the public cloud using the private cloud to view uploaded document in order to verify, if the document is correct then the verifier body prepares a new document called FINAL CER-TIFICATE consisting of user name, address and all required data for the certificate then it sends to the signer body in order to get signed to the certificate. If the uploaded document is not correct then it is rejected by the verifier entity and he guides the public cloud server to send a notification message to particular user i.e. your uploaded document is incorrect, please provide correct proof.
Stage 4: In this stage the signed certificate is sent to the public cloud server and notification message send to the particular user i.e. your income certificate is ready and collect by downloading in our website by providing the unique identity code.
Stage 5: In this stage all notification messages from the public cloud server will be delivered to particular users mobile and the users also allowed replying their feedback.

N.M.Musee [5], in 2015, the study proposed to develop a cloud based system for the authentication of academic certificates in Kenya. The author developed a prototype that enables a collaborative interaction among prospective employers, certificate holders and legal certificate academic certificate issuing institutions. The prototype works using the cloud computing technology. This application is hosted in the private cloud as SaaS. Furthermore, the author stated that cloud computing environment is preferred to deploy the developed prototype due its capability to make available the application from any device that contains a browser by using the internet. Therefore, this authentication system is accessible online by employers, students and academic institutions by using web content viewers. The database of this application is also deployed on the cloud computing to enable an academic certificate authentication as needed. One of the concerns of the cloud computing environment is data integrity and security. However, the author implemented the

role and authorization techniques to enhance data integrity and security in the cloud. The design and the development of this cloud based authentication system plays a significant role to the body of knowledge of the cloud computing and to research area of the document authentication technologies. In addition, the contribution to reduce the use of fraud document takes a large percentage.

M.Kumar et al [20], in 2015, the main objective of this document is to create or implement the central e-governance framework that is beneficial or profitable for the Indian government. Through this model, all government organizations and agencies will effectively and conveniently exchange data and information. The purpose of this model is the use of ICT infrastructure, providing services between architectural models of e-governance and providing central connectivity to the various government departments of the Government of India. The aim of the proposed model is a faster and more reliable exchange of information, integration between ministries and the best communication between all departments.

The central architecture framework for electronic governance is the interactive model that integrates India's center, state, block center, and entire gram panchayat, providing a better information delivery service between the central and state levels. Under this approach, communication between the center and the state will be flexible, cost-effective, and provide the best connectivity for all Indian government departments. The purpose of this framework is to centralize the entire IT department in an organized framework and for e-governance, reducing the initiative's integration method.

This architectural framework for the e-governance system covers cities and rural areas, making it easy to connect the user nationwide and integrate the national e-governance plan with the ICT infrastructure and e-governance process, electronic authentication. This framework provides useful coordination between the center's office to display and increase the district, block, or gram panchayat in a cost-effective manner and reduce the integration problem. All departments in India communicate effectively with a single framework and reduce communication costs.

Ghazali and Saleh [3] proposed a model-based approach for the implementation of cloud computing frameworks for graduation certificate authentication, to reflect the way in which employers function in terms of the authentication of degree holders that apply for job by a collaborative platform that creates a conducive environment to interact with various educational

institutes that are entitled to provide various levels of qualification certifications. It reflects how to overcome the problem of using fraudulent academic documents to get a job offer.

It also discusses how to transform traditional authentication into electronic authentication based on the cloud and how users can easily use electronic documents and improve authentication processes during employment recruitment. The authentication of graduation certificates is a challenge for the verifier (the prospective employer who wants to verify the certificate). To address this issue, a cloud-based model for certificate authentication is proposed. The university, the graduate and the verifier are the three parties involved in the proposed solution in order to accomplish accurate certificate authentication. Three key aspects security, validity and confidentiality are considered in the proposed model.

Several internal and external benefits can be obtained by using the proposed model. Internal benefits include improved work processes and ease of use for university staff due to the digitization of the authentication process. External benefits include the receipt of faster and more efficient authentication results by students/alumni and employers. The proposed model could also improve the links between universities and government entities.

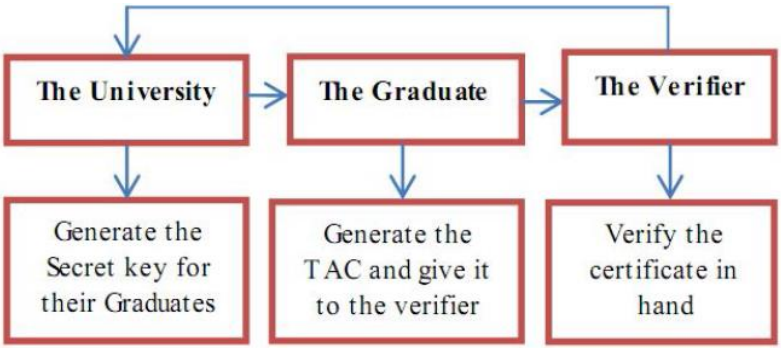


Figure 2. 6: Suggested process for certificate verification [3]

The proposed model transformed traditional computing into cloud computing by introducing the concept of cloud computing in graduation certificate verification, performing security, validity and confidentiality evaluations, designing a cloud computing model, evaluating it, establishing an implementation strategy. Several methods can be used to verify a document and can guarantee the originality and confidentiality of a document, including cryptography techniques and cloud services [5], [16]. Both cryptography techniques and cloud services are incorporated into the suggested solution.

According to the paper in [28], the new, dynamic and emerging ICT technology, the cloud computing technology can be used to store documents and enable users access them on demand using an android application. The researchers developed an application called I-Docket or wallet based application for storing multiple personal documents in a remote cloud server multiple personal document owners can scan and store their documents through their document issuers or verification authorities. After having stored the documents, users that have smartphones can login and request for QR code based on selected document category for later document authentication purpose while users that do not have smartphones are provided a unique ID that can be used for retrieving documents. This is considerably essential to minimize the insecure way of carrying multiple personal documents. More importantly, any user that have a smartphone can scan the QR code to retrieve multiple documents at once which actually results in saving much amount of time. Therefore, this research work has done an intensive effort towards the safety to user documents and the retrieval of them with minimum response time. The authors has clearly studied and identified the concerning issues of carrying multiple physical documents. They explained that portability and safety are the main worrying problem. To solve all the aforementioned issues during carrying of multiple documents for identity proofs and other several transactions, the researchers introduced a new concept, the I-Docket which reduces the need to carry multiple printed documents thereby providing a security mechanism for a safe transactions with them. I-Docket is an android application that contains a combination of multiple documents and identification proofs that enables personal identification, authentication, data storage and application processing. Furthermore, the authors has stated the limitation of I-Docket regarding to storage space and data transfer speed. As a result, they suggested that building an efficient system is important. The core objective was to develop an application that incorporates multiple documents of an individual user.

The I-Docket contains four components:

1. Admin (Server System): admin is responsible for managing the authorized person that can scan and upload documents on behalf of the document owner users to the cloud storage. The cloud storage can be also considered as the admin.

2. Authorized Person: the authorized person role is to manage multiple documents of individual users in the cloud storage. They help to move all data and documents of the users to the cloud storage.

3. Android Scanner App: Android Scanner app is used to scan the QR (Quick Response) code for retrieving all documents related to a particular user. It can also impose penalty for those users who are found guilty.

4. User Application: User application is used to generate the QR (Quick Response) code based on selected category of the documents. This application also enables users to do money transactions online.

Security is enhanced by the use of only authorized access to the documents. The QR code provides safety to documents of the user.

To summarize the related research, all the above researcher has discussed on the problem of the manual printed documents authentication such as academic documents, and how to solve this traditional way of verification of issued documents. However, the first four works have not used the QR technology which is the most commonly used, fast and cost effective mechanism for authenticating documents. On the contrary, the last paper has developed and designed a cloud based verification models and prototypes on the basis of QR code though there are limitations on the security and integrity of the proposed frameworks. The QR code is not secure by itself that it needs the implementation of cryptography technology to keep the integrity and security of the encoded data. They have not introduced the widely used authentication mechanism that makes use of the combination of QR code and digital signatures technologies. As a result, we proposed to develop a flexible, cost effective and secure cloud-based electronic authentication/verification framework that enhances communication between the potential employer sectors and certificate issuing institutes there by reducing the use of fake credentials to gain personal benefits. More importantly, this enables fair employments for all citizens, better quality of public services, building of confidence and reputations of employer and certificate issuing organizations.

Another, the above researchers have also done much efforts that improve customer satisfaction customer services and customer service provision. They listed several problems and propose solutions for those problems as we have seen above. Nevertheless, none of those researchers have

introduced the selection of cloud platform, service provider, the framework or architecture to solve the problems related to document verification such as documents of graduation or to communicate government with employee (G2E). In addition, some of them also have not implemented the most important authentication technology the machine readable code, QR code that can be secured by the use of digital signature. Furthermore, data transfer across the cloud computing environment is a considerably concerning issue regarding to security and integrity. However, most of the papers have used a role based authentication which is still fall prey attacks from intruders. Hence, to provide a secure data transfer between parties through the cloud computing environment that works on the basis of internet the researcher of this study has used the JSON Web Token (JWT) technology.

Table 2. 3: Comparison of the related paper and the proposed cloud based framework

Title	***Achievement***	***Gap Analysis***
An academic certification verification system based on cloud computing environment: ***N.Musee***	Developed a cloud based prototype to verify academic certificates.	• The researcher did not discuss how to evaluate to select the cloud service providers. • He did not implement a secure QR code and JWT for an efficient and safe way of data transfer between parties.
Cloud Based Graduation Certificate Verification Model: ***G.Osman, S.Omar S.***	developed a model for the verification of graduation certificates by using a cloud service and cryptography.	• The researcher did not discuss how to evaluate to select the cloud service providers. • They did not also discuss any point related to the use of secure QR code and JWT for an efficient and safe way of data transfer between parties.

Central Architecture Framework for e-Governance System in India using ICT infrastructure. ***M.Kumar, R.Bhatt and K.Singh***	Model most of government agencies and organizations will interact effectively and conveniently share the data and information.	• Not specified cloud computing architecture, model, and platform. • A proposed cloud computing architecture, and service delivery model. • They did not also consider fraud preventing technologies such as QR code and digital signature.
Develop the Cloud Based Personal Document Storage System and Retrieve Them Using QR Code: ***W. Ashrut, S. Pritesh***	Developed an android based I-Docket application that scans and stores multiple personal documents in a cloud storage to reduce carrying multiple documents and security of documents.	• Even though the authors have implemented the QR code for a fast retrieval of documents, they did not identify the insecurity of the QR code. • They did not also discuss about the selection criteria of cloud services and platforms.
Secure Higher Education Credentials Framework using cloud computing concept in Ethiopia (proposed own work)	Design of a secure higher education credentials authentication framework in Ethiopia and prepare and place a prototype in a remote cloud server as a service	• Most service delivery infrastructures are not implemented. Therefore, it takes longer time to evaluate and finalize all functionalities of the system.

Chapter Three: Research Methodology

3.1 Introduction

The Cloud-based E-authentication and E-governance frameworks were studied to propose the highly secured and scalable cloud-based E-authentication framework for issued graduation certificates from higher education institutes(HEI) to transform the current traditional way of document authentication to highly sophisticated electronic authentication in Ethiopia. The researcher started the study by conducting interview and questionnaire with employees of purposively selected HERQA departments in Addis Ababa as a representation of the whole country to collect data about the current methods and challenges faced on the process of academic document authentication during applications for various purposes.

Based on these steps, a design of cloud-based E-authentication framework and its prototype were developed to address the problem in (Figure 3.1).

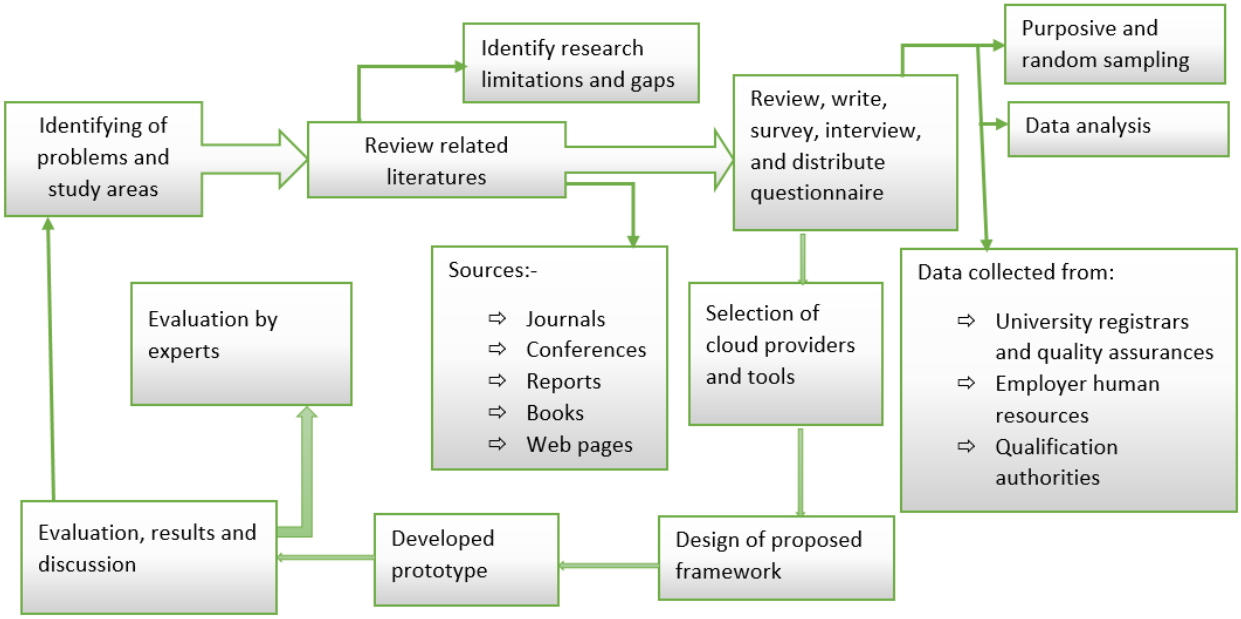


Figure 3. 1: Research Methodology

3.2 Research Design

A large number of research studies have been employing one of the three commonly used research approaches, which are design oriented, quantitative, qualitative, and mixed method [29]. The

quantitative research approach uses standardized measures, numerical values, have large sample size, and analyze data using statistical program. It is applicable to phenomena that can be expressed in terms of quantity or number [30]. On the other hand, qualitative research approach is focused on describing situations, phenomenon, problem, or event; tends to be more in-depth and have smaller sample size [31]. A mixed methods research design is a procedure to analyze, collect, and mix research and quantitative and qualitative methods in a single study to understand a research problem [32].

Design-Oriented Research creates an artifact by artificial object and its basic objective is producing new knowledge during this process. It is mostly focus on knowledge flows and process steps that is problem awareness, suggestion, development, evaluation, and conclusion; eventually aims to get result or output [33].

In this study, a combination of qualitative and design oriented research method were used for data manipulation and to evaluate the functionality of the prototype. To demonstrate the usefulness of the proposed E-authentication framework for higher education credentials by prospective employers, the design-oriented research methodology was used in this study. Design-oriented research method is a problem-solving model [34]. The five steps of design-oriented method followed in this work are identification of problems and requirement, framework design, framework evaluation, revaluation and improvement of framework, communication, and discussion of research.

3.2.1 Identification of Problem and Requirement

Currently, various potential employers, employer agents, and higher learning institutes are using the traditional way of authentication for documents of job and higher level education applicants. As a result, there is no central institutional knowledgebase, no effective way of working together, and communication channel. In general, the tasks of authentication for those job and education seeking individuals' qualification credentials are ineffective, cumbersome, prone to fraudulent practices and time consuming. To solve these problems, the requirement or data collection was the basic step to design the proposed framework after identifying the problem.

In this research study, the required data and user needs were collected using a variety of methods, including interviews with employees of HERQA. In particular, IT professionals, quality assurance and quality audit senior experts are main participants of the data collection process. Observation

with the study area and distribution of questionnaires with questions about the authentication of higher education credentials and problems encountered. Then the collected data was organized and analyzed to use for the design of the framework.

3.2.2 Framework Design

The design of the E-authentication framework focused on the elements or components from the performed literature reviews, observations, questionnaires and interviews to achieve the goals given under the given constraints and limitations. To design the proposed framework, reference architectures, models, frameworks, a web application architecture, for the Microsoft platform, paper document verification technologies, authorization technologies, android applications and other Internet resources were used.

3.2.3 Framework Evaluation

In the software development process, the framework can be evaluated at the early stage or later stage. This is used to compare and identify gaps in various alternatives during early design stages. There is different software evaluation architecture that includes experience-based, simulation-based or prototyping and scenario based [35]. In this study, the early assessment phase and prototyping are good, as the cost of remedying an error during the requirements was determined. The evaluation and improvement of the E-authentication framework was conducted based on a given quality attributes with the help of software development experts, systems development companies, and selected cloud technology experts, as presented in Chapter 6.

3.3 Prototyping Software Development Methodology

In software development, to produce the software product it passes through several steps and activities. There are various software development methodologies that follow a specific processes to deliver the final software product. For instance, Prototyping, Unified Process, Incremental, and Agile are some of the methodologies for software development. We can rarely combine process models or use together in software development process [36]. In this study, prototyping model was used to achieve the overall objectives.

Prototyping is one of the development process model to improve the design and execution of software projects by developing executable software systems (prototypes) for experimental

purposes. It is very suitable to gain experience in new application areas and to support the development of evolutionary software [37].

Therefore, prototyping is a process model that provides a solution to the problem, and it is the practice to create an early version of a system that shows certain features of the actual system. There are two basic types of prototyping, which are throwaway, and evolutionary prototyping. In throwaway prototyping, the various parts of the system are developed and then ignored after demonstrating the basic functions that the system will perform. Therefore, the final system to be delivered will be different from the prototype.

However, evolutionary prototyping technology implements the prototype of the system, demonstrating its basic functions, and will ultimately be part of the final system that can be delivered. Therefore, we used the evolutionary prototyping method for the proposed study.

3.4 Data Source

The data used as input for this work were collected from the following sources:

- The primary data source is to use interviews and questionnaires in targeted quality assurance agency, HERQA which monitors and regulates both private and public higher education institutes in Ethiopia. Employees of permit, accreditation, and authentication issuance and ICT professionals are selected for the survey of this research study.
- The second data source in this work is a comprehensive literature search and document analysis from the Internet. Therefore, the Internet is one of the data sources, as explained in the methodology section in the first chapter.
- The other data source in this work was the observation. During this study, observations were used as a means to gather the required authentication tasks, specifically to know the most repetitive and paper-intensive process, delays in transporting documents and letters and understand coordination across departments, and too many manual authentications and checks.

3.5 Sampling Techniques

Both private and public employer companies and higher education institutes (HEIs), recruiting agencies, quality assurance (QA) agencies and prospective employees are the major stakeholders in the verification and authentication process for credentials. However, the autonomous QA agency, HERQA bridges all the other stakeholders by taking the responsibility of authentications and accreditations [38] for credentials, HIEs and their programs.

Therefore, in this research study, the sample selection includes the selection of individuals from HERQA employees and purposive sampling [39] was used to collect the data. As depicted in Figure 3.2 below, HERQA consist of 3 deputy director generals, 17 directorates and 2 offices.

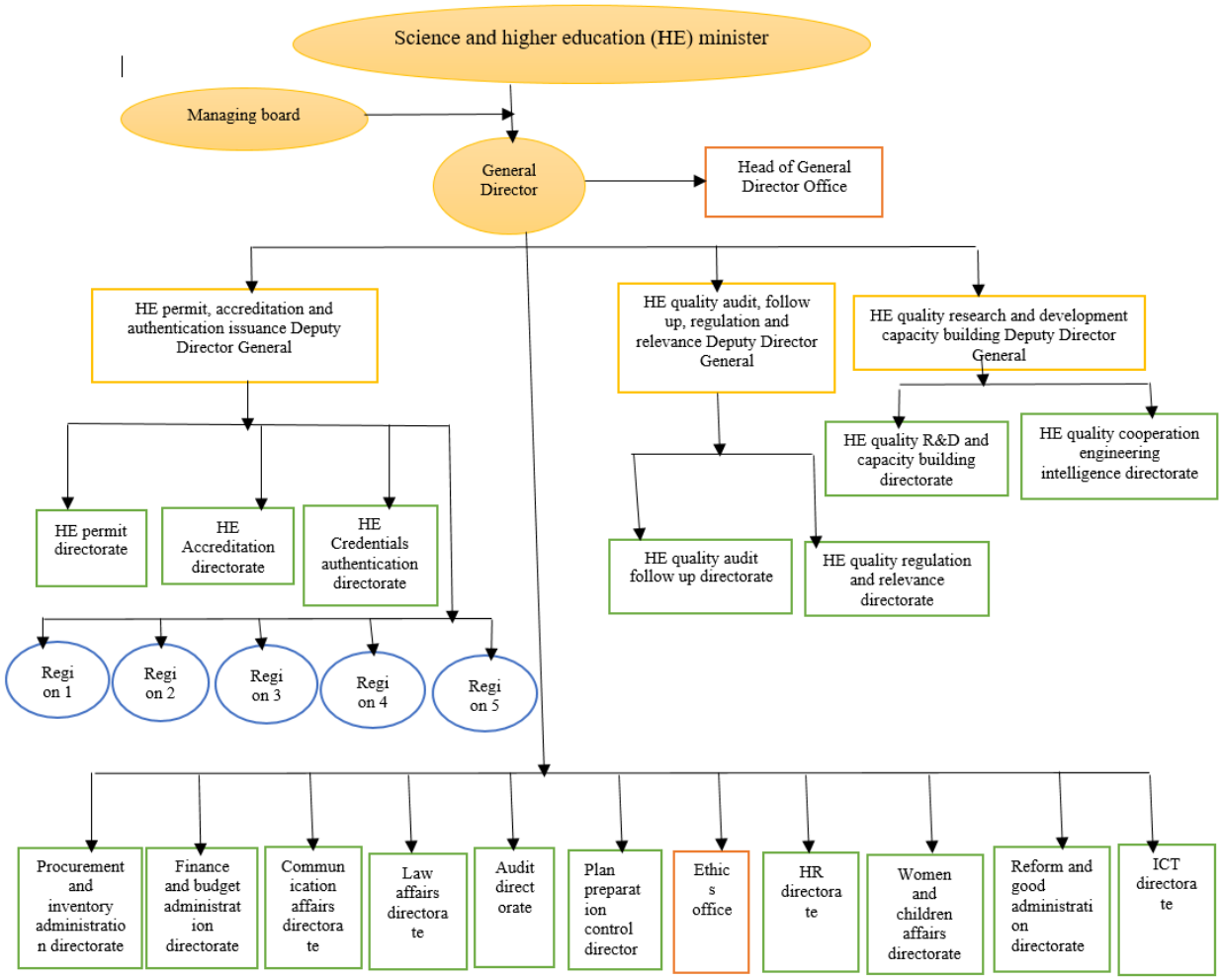


Figure 3. 2: Organizational Structure of HERQA

In this research study, purposive and random sampling technique were employed to collect the qualitative data. Therefore, data collection was started by identifying the participants using purposive sampling technique. Before distributing the questionnaires and carrying out the interviews, the participant organizations and departments were identified. Firstly, the researcher identified the target organization to be HERQA. HERQA was selected because of its responsibility to give authentication of higher education credentials and accreditation of higher learning institutes and their programs.

Secondly, the target departments were identified as HE permit issuance directorate (HEPID), HE accreditation issuance directorate (HEAID), HE credentials authentication issuance directorate (HECAID), and ICT directorate. Accordingly, the target population was set to contain 10 permit issuance experts, 10 accreditation issuance experts, 20 credential authentication experts, and 10 ICT experts.

In general, this was resulted to a target of 50 respondents in total. This sample was used as a representative to the entire country to design and develop a secure and cloud based framework of higher education credentials authentication digitally.

3.6 Sample Size

In this research study, we selected a total of 20 respondents by using stratified random sampling strategy. These respondents includes employees of HERQA in the four directorates, HEPID, HEAID, HECAID and ICT that are situated in Addis Ababa. This sample size was appropriate because the respondents were involved directly in the verification and authentication process of claimed higher education credentials by education or job seeking applicants.

Table 3. 1: Sampling Population Size

No	***Directorate***	***Total Targeted Population***	***Sample Size***	***Counted***	***Response Rate in (%)***
1	HEPID	10	4	4	100
2	HEAID	10	4	4	100
3	HECAID	20	8	6	75
4	ICT Experts	10	4	3	75
	Total	50	20	17	85

As we have seen from the above Table 3.1 the response rate from the respondent around 85 %. This shows that some of the distributed questionnaires were missed.

3.7 Data Collection Techniques

Research differs in a number of ways, but they have some similarities. One of the common aspects is the need to collect data. This data collection task involves three phases:

1) **Interviews**: In depth interviews were conducted to a total of 5 respondents, 1 deputy director general and 4 directorate directors about higher education credential frauds, current situations, barriers and solutions to the forgery practice.
2) **Questionnaires**: The questionnaire addressed a number of issues related to higher education credentials authentication tasks.
3) **Observation**: Observation tasks in Appendix C: Observation on Services, observed based on workplace study on HERQA for three days. In addition, we are part of a higher education institution and we observe the challenges on current manual system as a way to authenticate academic documents, non-important steps during the authentication process, its efficiency, and effectiveness of the current system, technology adaptation and the knowledgebase. This is done through different techniques, but getting the right information was extremely difficult, as observed.

Using the questionnaire, we examined the efficiency and effectiveness of the current manual system, the type of delivery services, the problems they face with the current system, and the possible solutions to the current problem and employers' interest. It would be an electronic authentication on the basis of Cloud-based implementation. We collect data about these concepts because they help us to build the foundation for the design of the framework.

Chapter Four: Design of Proposed Framework and System Architecture

4.1 Introduction

This chapter describes the cloud framework based on the proposed framework. In order to design this framework for the provision of the software as a service, we have added ideas or concepts from IBM CCRA [46], NIST Cloud Reference Architecture [47], Microsoft Web Application Architecture [48], and available literatures on software architecture approaches for cloud-based systems.

In addition, from the Interview, Questionnaire, and Observation data analysis or result data from respondents are used as input data to determine and identify the components of SHECAF in the framework and architecture. The collected data helped to identify the current techniques, challenges, what the verification process involves, and how important will be the design and development of the proposed framework.

The CCRA reference architecture categorizes cloud business models and corresponding architectures based on seven cloud customization patterns. It identifies common architectural patterns for each cloud-adapted pattern that describes the technology that underlines every type of cloud implementation. The reason why we used these three reference architectures is:

1) It shows a way to construct the framework across all delivery models by providing the steps we follow and the time required to complete the components required save up.
2) It meets the required cloud requirements such as elasticity, self-service and flexible sourcing.
3) It uses comprehensive architectural principles to ensure design scalability for efficiency, security, service management and virtualization, as well as reducing errors throughout the development process.

In addition, we have used graphical elements or symbol representations of icons for cloud applications [23], which presents a collection of patterns to describe cloud computing, its service models, its deployment models and its architectural patterns in general. For this reason, they have cited three types of architectural patterns for cloud applications, such as elasticity patterns, availability patterns, and multi-tenancy patterns.

Moreover, we want to introduce a cloud-based E-Authentication of higher education credentials framework with two major parts: frontend and backend: which are usually connected via the internet. The first part presents HERQA and employer's infrastructures such as computers, laptops and the network used to access the cloud-based E-authentication management software as a service. The first part consists of the visible interface and applications (for example, web browsers like Chrome, IE, Torch, Opera, or Mozilla Firefox) that are needed to access the E-authentication software as a service from the cloud providers. The second part will illustrate the basic components and services of the educational credentials E-authentication system, which is the cloud part of the framework. These include various servers, middleware, storage and virtual machines, programming languages, platforms, E-authentication software as a service itself, security, tools, integration, and deployment models.

4.2 Data Analysis

Questionnaire and interview are a structured technique used to collect primary data to decide how to collect replies, questionnaire design, and analyze data after identifying the population and sample [35 - 37].

The techniques are focused on collecting input data that can help to the design and development of a secure smart authentication environment for the higher education credentials in Ethiopia, the efficiency, and effectiveness of the current manual system and how to forward the paper documents, currently how they are deployed, and what efforts have been made to make it available to you one after another. In addition, how the institution handles a variety of authentication request, authentication processes related to technology, collaboration, and knowledgebase environment.
To know how many employees of HERQA respond, the total number of in the Appendix B: Questionnaire Questions, distributed 20 and 17 returned from respondents.

Table 4. 1: Questionnaire Response

No	***Questionnaire List***	***Choices***	***Counted***	***In (%)***
1	Current authentication method	Manual authentication	14	82.35%
		HE databases	0	0%
		National databases	0	0%
		Other	3	17.65%

2	Response time of current authentication method	Two days –five days	5	29.41%
		Six days – ten days	8	47.06%
		More than ten days Fifteen days	4	23.53%
3	What are the authentication parameters used in the current technique?	Issuer name	17	100%
		Program	17	100%
		Logo	17	100%
		Issuer seal	16	94.12%
		Issuer signature	10	58.82%
		Credential holder name	17	100%
		Course	15	88.24%
		Year of entry	17	100%
		Year of graduation	17	100%
		Grade	17	100%
		Other	7	41.18%
4	Does your agency has a common standard and framework for the authentication of higher education credentials?	Yes	1	5.88%
		No	16	94.12%
5	Is there any sound mechanism to trace the status of authentication progress?	Yes	1	5.88%
		No	16	94.12%
6	Does the current authentication method has any easy way to locate authenticated credentials?	Yes	3	17.65%
		No	14	82.35%
7	Is there any platform to report/inform fraud cases from various stakeholders?	Yes	5	29.41%
		No	12	70.59%
8	Cases of lost credentials	Never	7	41.18%
		Not so often	10	58.82%

		Most of the time	0	0%
		Always	0	0%
9	Cases of faked credentials	Never	2	11.76%
		Not so often	9	52.94%
		Most of the time	6	35.29%
		Always	0	0%
10	Challenge of the current authentication method	Time consuming	15	88.24%
		Costly	16	94.12%
		Unavailability of responsible officers	10	58.82%
		Inability to detect fraud	7	41.18%
		Other	2	11.76%
11	Effect of using fake credentials	Socio-economic failure	17	100%
		escalation of illegal practices and corruption	14	82.35%
		Damage of reputation and income	14	82.35%
		Lack of trust and declined education quality	17	100%
		Other	3	17.65%
12	What is your level of satisfaction in regard to the efficiency and effectiveness of the current authentication method?	Extremely high	0	0%
		Very high	0	0%
		High	4	23.53%
		Low	13	76.47%
13	Do you think the implementation of E-authentication system in your agency will enhance the security and integrity	Yes	17	100%
		No	0	0%

	of credentials and the efficiency and effectiveness of the authentication task?			
14	Do you recommend the adoption of cloud technology for the implementation of an E-authentication application?	Yes	14	82.35%
		No	3	17.65%

4.2.1 Authentication Methods of Higher Education Credentials

The author of this research study asked respondents of the survey about the methods that are currently employed to authenticate higher education credentials. As a result, we were able to know the most common used ways of verification and authentication of higher education credentials used by HERQA. Accordingly, as shown in the Figure 4.1 below 82.35% respondents indicated that manual authentication of higher education credentials were carried out in their organization while 17.65% indicated other methods of authentication were used such contacting through emails, letters, informers and phones.

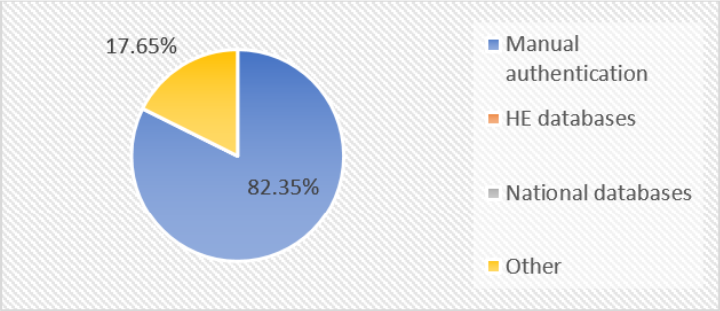


Figure 4. 1: Authentication Methods Used in HERQA

4.2.2 Time Taken to Authenticate Higher Education Credentials

From the questionnaires distributed to investigate the time taken to get authentication results of higher education credentials from universities, we found that it takes minimum of two days and maximum of two weeks were needed to obtain a response from higher institutes to employers.

4.2.3 Authentication Parameters

The researcher performed a survey on the criterions for authentication of higher education credentials. Most of the participants of the survey indicated that issuer name, issuer program, issuer programs, logo, seal, signature, credential holder name, grade, graduation year and entry year common authentication parameters. Moreover, degree types, holder enrollment ID, card ID and

age were also cited as authentication requirements in the others category. Figure 4.2 shows the various authentication parameters.

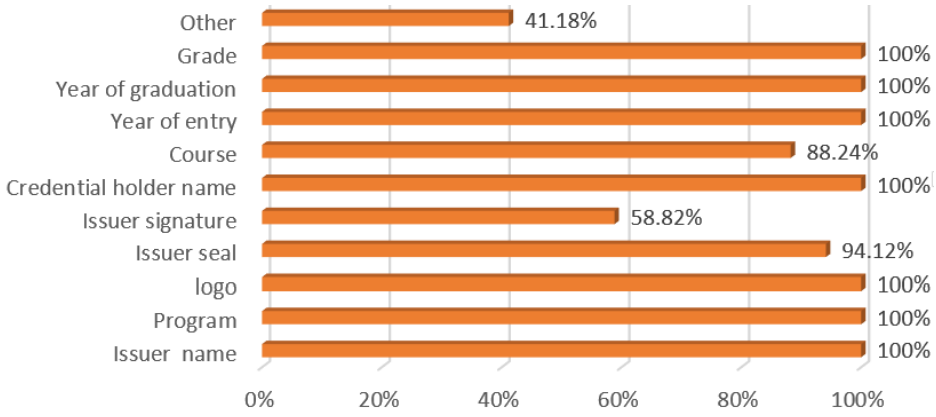


Figure 4. 2: Criterions for Authentication of Higher Education Credentials

4.2.4 Easy Standards, Frameworks and Mechanisms of Credential Handling

Respondents were asked to indicate if there is any common standard and framework in their agency that enables to locate credentials and trace status of progress easily. However, as the response in table 4.1 illustrated, 5.88% respondents indicated that there is common standard and framework of authentication credentials while 94.12% respondents indicated No for that. Moreover, in regard to the availability of an easy way to detect the status of authentication progress 94.12% of the respondents indicated there is no while 5.88% of the respondents indicated on the contrary. Similarly, respondents were asked to indicate if there is any easy technique that helps to locate credentials and report fraud cases and 82% and 70% of the respondents indicated that there are not respectively.

4.2.5 Cases of Higher Education Credentials were Lost

Respondents were asked if they had ever faced a missed higher education credentials during a request for an authentication. Most of them indicated that it was not so often to confront such cases in their agency. However, 41% of the respondents also indicated that they never faced cases of lost credentials.

4.2.6 Cases of Faked Higher Education Credentials Caught

The respondents were asked to indicate whether they have ever had a faked higher education credentials during authentication. As the respondents response tabulated in table 4.1 more than

50% indicated that cases of faked credentials are not so often happened, 35% of the respondents they have had most of the time, and 12% of the respondents indicated they have had never. In general, most of the respondents indicated that they have cases of faked credentials during the authentication of higher education credentials.

4.2.7 Challenges of the Current Authentication Method

Respondents were asked to indicate the challenges of the current authentication methods and most of the respondents indicated that the current method of authentication is time consuming, costly, unable to access responsible officers and it has no mechanism to detect fraud while few respondents also indicated insecurity, worn out cases, lost cases and efficiency as another challenges of the current authentication technique. Figure 4.3 illustrates the distribution of the response of the questionnaire survey in regard to the challenges of the current authentication system.

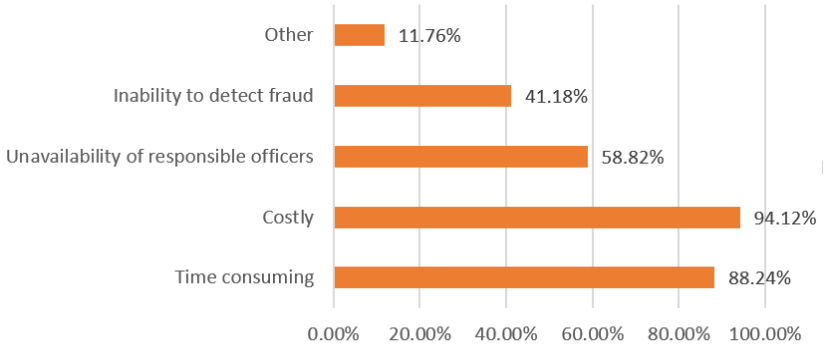


Figure 4. 3: Challenges of the Current Authentication Method

4.2.8 Effect of Using Fake Credentials

The effect of using fake credentials were investigated from participants of the questionnaires survey and respondents of this survey indicated such as socio-economic failure, escalation of illegal practices and corruptions, lack of trust and declined education quality, damage of reputation and income. Moreover, other effects such as damage of competitiveness and public quality service, and unfair employment were indicated. Figure 4.4 shows the various effects of using fake credentials.

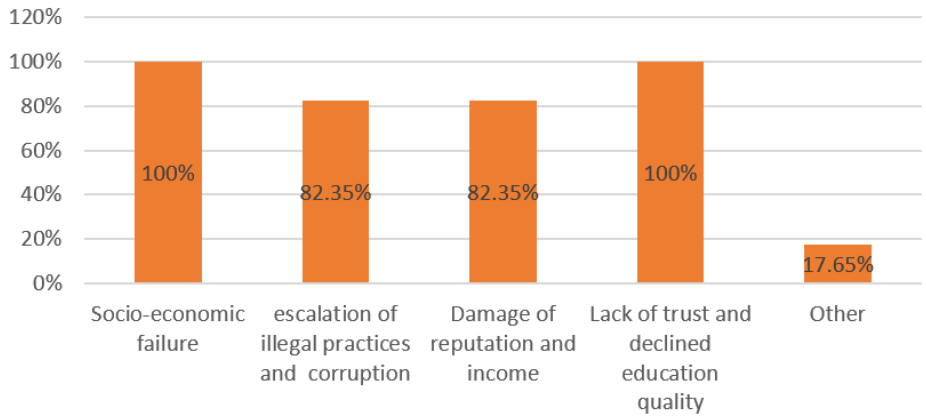


Figure 4. 4: Effects of Using Fake Credentials

4.2.9 Level of Satisfaction on the Current Authentication Method

Respondents were asked about their level of satisfaction on the current method of authentication and 76.5% of the respondents indicated that their level of satisfaction is low in regard to the authentication method that is currently in use.

4.2.10 The Implementation of E-Authentication as a Solution

As the response in table 4.1 shows respondents were asked to indicate their confidence in E-authentication application to solve the challenges of the current authentication method which is the manual way of authentication credentials and all the respondents believe that proposed paperless authentication technique can overcome pitfalls of the manual verification system.

4.2.11 Recommendation for the Adoption of Cloud Technology

Respondents were asked whether they recommend the adoption cloud computing technology for the implementation of the newly proposed E-authentication system or not and 82.35% of the respondents recommended the adoption of cloud computing for the implementation.

4.3 Selection of Models, Platforms and Tools

4.3.1 Introduction

This chapter provides an overview of the selection of cloud framework, platform and deployment model to implement the proposed E-authentication prototype, the comparison of three Major cloud platforms and the detail the Microsoft Azure platform for this work. To develop the prototype of the proposed framework, we started to find the best cloud platform to deploy our prototype as

software as a service (SAAS). In addition, we performed a depth study of the difference on the benefits between cloud and traditional framework for implementing our proposed and developed prototype. As a result, we have done an advanced search to compare and analysis cloud platforms, cloud benefit, cloud limitations, and other implementation tools to use the best for our purposes. This chapter also contains a selection of tools to design the proposed framework and to implement its prototype for the purpose of testing and evaluation purposes.

4.3.2 Cloud Deployment Models

Various world wider organizations use one of the following deployment models to move their business processes to the cloud environment [5].

a. Public cloud: services such applications and storages available over the internet publicly based on pay per use mode.
b. Private cloud: delivers services and customization capabilities to a particular organization only based on authentication and authorization access.
c. Hybrid cloud: uses a combination of private and public clouds
d. Community cloud: this is where resources of cloud shared among various communities of the same domain.

Deciding which deployment model to use for a particular business process is a significantly important to perform a depth investigation into the cloud deployment models and the nature of the business process to be moved into the cloud environment [16]. Table 4.2 below shows the comparison on the widely used deployment models.

Table 4. 2: Comparison on Deployment Models [21], [23], [24]

Parameters	**Public cloud**	**Private cloud**	**Hybrid cloud**	**Community cloud**
Security level	Low	High	medium	High
Cost	Low	High	Medium	High
Performance	High	Low	Medium	Low
Multi-tenancy	High	Low	Medium	Low
Agility	High	Low	Medium	Low
own control	Low	High	Medium	High

Location	Off premise	Off premise or on premise	Off premise or on premise	Off premise or on premise
Owned by	Cloud service provider	Single organization	Both	Organizations or cloud service providers

The major concern to use cloud environment is the privacy and security of data [5]. The comparison on the deployment model for cloud resources in table 4.2 shows that the private cloud more secure and enables best practice of control over one's own data. As a result, because of the electronic authentication of higher education credentials has a highly sensitive and critical business processes and data it needs a deployment model that provides high security and control management frameworks. Thus, the private cloud computing was selected as an appropriate and suitable model for deploying our proposed E-authentication of higher education credentials.

4.3.4 Cloud Platforms

PaaS is a cloud designed for software developers to develop web and mobile applications. In this study, we focus on the platforms used for web development and hosting that can communicate with mobile applications through a secure RESTFUL web service, WebAPI. There are many tools for application developers in the cloud environment, and we try to describe the most popular platform providers and their development and hosting tools.

In this research study, we compared and analyzed the three leading cloud platforms Microsoft Azure, Amazon Web Services, and Google App Engine to choose the suitable and better hosting and development averment for our application. From these platforms, we selected Azure platform for the deployment and development of our application.

When comparing the platform providers and their tools described below, we used evaluating criterions such as Integration, application, and GUI support, compatibility and middleware technologies, programming languages, and applications, data, scalability, service model, pricing model, deployment model and availability. The list of cloud application development and hosting tools compared in this work is as shown in table 4.3.

4.3.3.3 **Microsoft – Azure**

Microsoft's Azure platform is a group of cloud technologies, currently being engineered and under development to enable usage of massive computing power packed within Microsoft's data centers around the world. The main components of Azure platform are .Net services, Windows Azure, SQL storage, and live services. In addition, Azure is Microsoft's cloud platform that offers the combination of IaaS and PaaS at one to suit the needs of customers, which is a foundation for running applications and storing data in the cloud. It enables developers to use any language, framework, or tool to build applications [40], [41].

4.3.3.2 **Amazon Web Service**

Amazon web service [42] is one of the leading cloud platforms that provides several cloud services such as computing capacity by Amazon Elastic Compute Cloud (Amazon EC2), storage by Amazon Simple Storage Service (Amazon S3), database management tools by Amazon Rational Database Services (Amazon RDS), core database functions by Amazon Simple DB, secure routing servers over the Internet by Amazon Rout 53 (Amazon scalable DNS), content management and distribution over the internet with high speed by Amazon CloudFront, and big data processing through a web service by Amazon Elastic MapReduce.

4.3.3.3 **Google - App Engine**

The App Engine is Google's platform designed for web applications and supports different languages such as Java, Python, Go, and PHP allows for integration to other technologies such as Hadoop, MongoDB and others. It uses a sandbox model, which isolates processes thereby reducing the risk that a rogue process on a physical server will disrupt operations of other processes on that server. Google App Engine like other platform manages many of the implementation details about maintaining virtual servers, operating systems, and development tools. Nevertheless, it is restricted to four programming languages, which is its limitation.

App Engine support of more languages will appear in the near future and is the SDK which completely emulates Google's server environment. This is useful because customers can create their applications locally, in real time, without uploading them. Then it comes the web based admin interface. This interface contains all the necessary tools to manage and debug user applications and isolates processes thereby reducing the risk that a rogue process on a physical server will

disrupt operations of other processes. Finally, the Data store API, which is the Google's scalable persistence layer [41], [43].

Table 4. 3: Comparison among the three major cloud platforms

Features	***Azure***	***Amazon Web Service***	***App Engine***
Support	- GUI and command line - Only in windows	- Both visual and command based interface - Cross platform	- Both visual and command based interfaces -
Compatibility	- Fully compatible	- Fully compatible	- Limited compatible
Frame work	Cake PHP, Django, etc.	Not supported	Django, Webapp2
Language support	.NET, Java, PHP, Node.js, Python, and Ruby	.NET, Go,Java, PHP, Node.js, Python, and Ruby	Java, Python, Go and PHP
Service	-Shared hosting -No dedicated virtual host -No virtual private servers -auto scaling -storage and development services -Databases(azure SQL) and database migration - server migration -better data transfer	-No shared hosting -dedicated virtual host - virtual private servers -auto scaling -storage and development services -supports RDBMS(but no SQL database) and database migration -server migration -best data transfer -application discovery -virtual private network -administration and	-No shared hosting -dedicated virtual host - virtual private servers -auto scaling -Storage and development services (but no hybrid storage gateway) - supports RDBMS(but no SQL database) and no support to database migration -no server migration -limited data transfer service -no application discovery

	-application discovery -virtual private network -administration and information protection	- no information protection	-virtual private network -no administration and information protection
Pricing	Based on size of instances running	Pay per use of resources	Based on usage, monthly bills or free usage
Availability as SLA	99.95%-99.9% uptime	99.99% uptime	99.99% uptime

Based on the above comparison and the analysis of Table 4.3, we used Microsoft Azure for our study to implement the prototype of the proposed architecture. Microsoft Azure automates basic systems management tasks such as provisioning, configuring, and scaling virtual servers. In addition, Microsoft Azure provides a wide range of environments (UI, command line, and .Net), flexibility, and access to various programming languages, including .Net will benefit us greatly.
Microsoft Azure provides agility and an open cloud platform that helps to grow the business with greater efficiency and responsiveness to change. With Azure, possible to quickly upgrade, scale or shrink as needed, and avoid high capital costs - you only pay for what you use.
Azure also works seamlessly with other Microsoft software and services, including Windows Server, SQL Server, Exchange, and SharePoint, to secure and protect the organization most important information. By comparing the Microsoft Windows Azure. It has a variety of languages and databases that allow the developer to make their applications easy and understandable. We can manage our code using a web portal.
The main criteria for choosing Microsoft Azure are;

Firstly, it provides the developer with more deployment options than the other three platforms and more sets of application programming interfaces (APIs).

Secondly, is that we are familiar with Microsoft products such as the Microsoft's Visual Studio (VS) Integrated Development Environment (IDE), Angular JS, and SQL storage. Therefore, for most popular cloud service providers uses Microsoft Azure.

Third, the upcoming releases of Azure are going to support applications written in languages such as Python and PHP.

Fourth, it resembles existing Windows environment a lot. In general, the migrating applications to cloud is easy. This partially stems from the fact that Azure's services exploited by an application whether it run locally or in the cloud. The developer can deploy locally using web deployments on IIS.

In addition, Microsoft has features like -

- High **availability** (99.9%) of the application and the data.
- **Open** and **flexible** cloud platform that enables to rapid creation, deployment, and management of applications in a global network of Microsoft managed datacenters.
- Possible to integrate public, private cloud applications with the existing IT environment and quick deployment of the application to new customers etc.…

4.3.4 Tools

Programming language: **-** We used the .Net framework to develop the prototype for the following reason: -

- We are more familiar with Visual Studio than other languages and it is an integrated development environment (IDE) from Microsoft.
- Used to develop computer programs for Microsoft Windows as well as websites, web applications, web services, and mobile applications, uses Microsoft software development platforms such as Windows APIs, Windows Forms, Windows Presentation Foundation, Windows Store, and Microsoft Silverlight [44].
- It can generate both native and managed code, and includes code that supports IntelliSense (the code completion component) and code refactoring. The integrated debugger works both as a source-level debugger and as a debugger at the machine level, supporting 36 different programming languages [45].

In general, various tools used to achieve this study. Some of the tools are Windows 10 operating system and Microsoft Office 2016 for the preparation of the document, Adobe Photoshop for creating images and other diagrams (Microsoft Visio 2016) used. As mentioned above, Microsoft Office, Excel, and Visio 2016 used because, used to create simple or complicated diagrams. The architecture implementation based on Microsoft Azure Platform and using the ASP.net based

Microsoft Visual Studio MVC architecture. The prototype used to demonstrate the architecture implemented with AJAX JS for the UI implementation and Microsoft Visual Studio (IDE) of ASP.net for the backend implementation has been developed and deployed on the IIS8 server.

4.4 Design Goals and Constraints

The main goal of the cloud-based E-authentication framework design is to provide E-authentication software as a service that meets the employer organizations regarding to the authentication of prospective employees' educational credentials. As a result, the framework should be flexible and easy to use, with increased productivity, a well-defined interface, and user-friendliness.

Constraints are a limiting factor and severely restrict options for making design decisions. In software architecture design, there are two types of technical and non-technical constraints or business constraints [49]. In this study, the following technical and non-technical constraints were considered.

Technical constraints include:

Programming language: - we have used .NET framework language to develop the prototype of the framework.

Platforms supported: - This study works properly on windows operating systems. Azure platform supports deployment of applications developed on Microsoft environment.

Non-technical constraints include:

Schedule: - this is the time frame for final delivery of the thesis work, so we have stuck with our schedule during this work.

Software and Cloud platform service provider licensing restrictions: - We are restricted to using freely available software and tools to perform a work that lacks full features like Microsoft Azure platform.

Internet-based: - all cloud-based applications are working properly on dedicated internet connection; Due to this, slow internet connection may affect the accessibility or availability of the system. In addition, it may be affect for deployment and development purpose.

4.5 General Cloud Framework for SHECAF

The central function of designing an electronic authentication framework based on the cloud technology is to create a smart and convenient ecosystem that makes the management of higher

education authentication processes easier and secure. The design and development of a distributed and shared institutional repository to produce an automatic authentication system for the most repetitive task of authentication of higher education credentials instead of the traditional way of verification will result in saving time and non-standard work avoidance, effective storage and accessibility, efficient credential tracking capabilities and intelligence function for all registered employers in Ethiopia. In addition, the process of designing a cloud-based electronic authentication framework will be progressive. As a result, the design of SHECAF according to the current state of E-authentication, cloud-computing expertise, and Microsoft Azure can learn about the following generic cloud framework, shown in Figure 4.5. It contains the components listed below.

Physical resource pool: These include hardware resources such as network, storage devices, and virtual servers. These are linked by network virtualization with the intention of creating cloud-centric university knowledge-sharing networks and sharing various documents and letters as well as various institutional forms.

Infrastructure as a service (IaaS): The delivery organization and end users can share the full hardware resources by virtualizing physical resources. Therefore, virtualization technology increases user demand by dynamically allocating resources to active demand, thus avoiding the use of fixed storage space. It is fully managed by the cloud provider and manages the resources and environment of physical infrastructures such as servers, storage, and networking to the virtual machine.

Platform as a service (PaaS): It contains the Microsoft Azure platform, which will control the development environment to enable creation and hosting of applications and programs with the ability to access private cloud resources and platforms.

Software as a Service (SaaS): End users order software as a service provided by the platform service providers over the network. The service providers collect payments based on used services. The SaaS's cloud based electronic authentication in Ethiopia have various services such as service delivery infrastructure, electronic authentication service such as: electronic fraud report, verification request, send / receive and forward/route documents, manage institutional knowledgebase, and messaging, escalation engines, design workflow, alerts and notification, SMS and E-mail exchange can be provided at this level.

Microsoft azure: As we have described in chapter four, it is Microsoft Azure offering. This platform used to create and deploy cloud-based electronic authentication system.

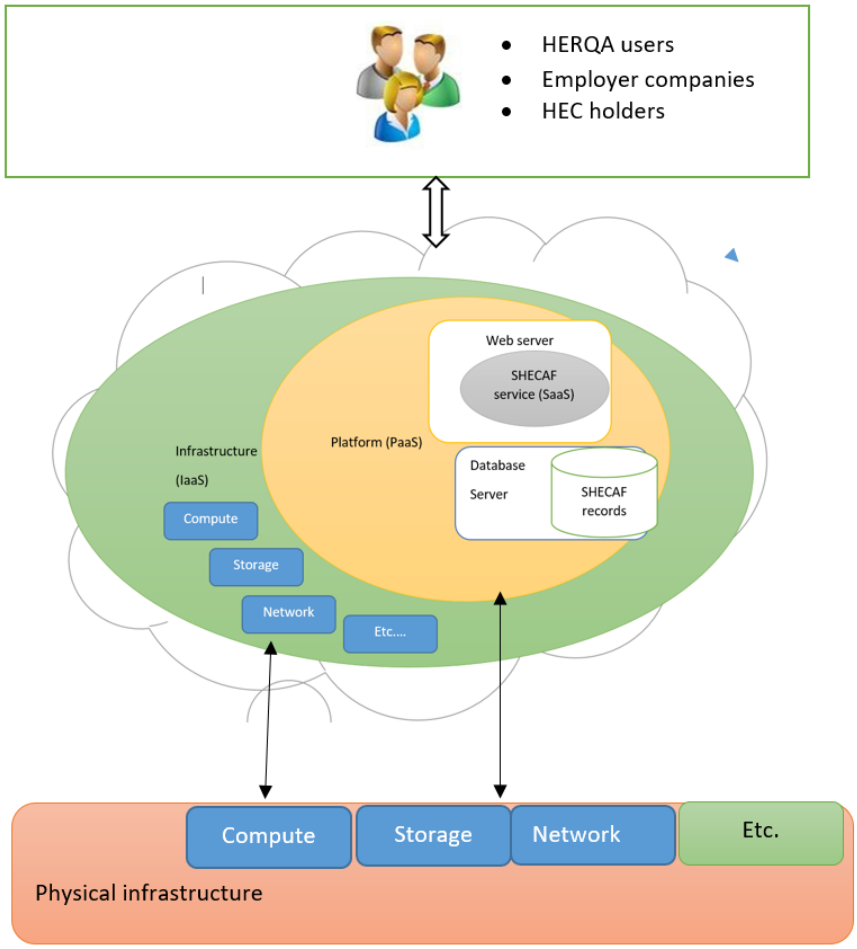


Figure 4. 5: Cloud Based Model of SHECAF

4.6 The Conceptual Framework of Cloud Based Electronic Authentication

Due to several factors, it is true that in their current situation, using ICT in HERQA is not efficient, especially for the authentication of higher education credentials which involves a big number of customers and which also needs a high collaboration among different stakeholders.

Therefore, in this study, we proposed a secure cloud-based higher education credentials authentication framework that makes use of as digitally signed QR code and JSON web token technologies (JWT). To get the layer first, we analyzed the cloud taxonomy and got a classification that relates to cloud computing like service type, middleware, and others. However, we do not know the relationship between classifications; we reviewed existing cloud computing

architectures, including the reference architecture for cloud computing, the IBM cloud computing reference architecture, the NIST cloud computing reference architecture, and the Microsoft Web Application Architecture.

The study proposes the following architecture to implement cloud computing as a tool and access the electronic authentication for higher education credentials. In addition, it is designed to realize the electronic authentication components, design workflow, integrate with other systems, use tools, and provide a worldwide electronic authentication.

Our cloud-based E-authentication framework includes the following features.

Application independence: to ensure that access to resources is not dependent on a single application.

Platform Independence: to ensure that access to resources is not limited to specific hardware platforms. This enables accessing of data from the cloud application any time and places by using any web tool or browser regardless of the underling hardware architecture.

Long Term Access: to ensure that resources can be obtained and retrieved over a long period of time.

Architectural Integrity: to ensure that the architecture for IT development is robust and can evolve in the future.

The institutional records and standards should be followed as well as authentication and role-based access in accordance with the institution's security standards. **Figure 4.6** shows in below, the framework for using the Microsoft web application and the cloud computing architecture. The framework is follows the overall Microsoft architecture for web application in which users and end-user devices interact with electronic authentication application that is hosted on the cloud. After the users have requested in the presentation and the application layer, request/response from the core services and the data layer based on WebAPI. Similar to that, the data retrieved from data layer to user interface request. The framework is the general concept that contains the various tools, E-authentication components, integration, security, and other external systems to integrate with proposed system.

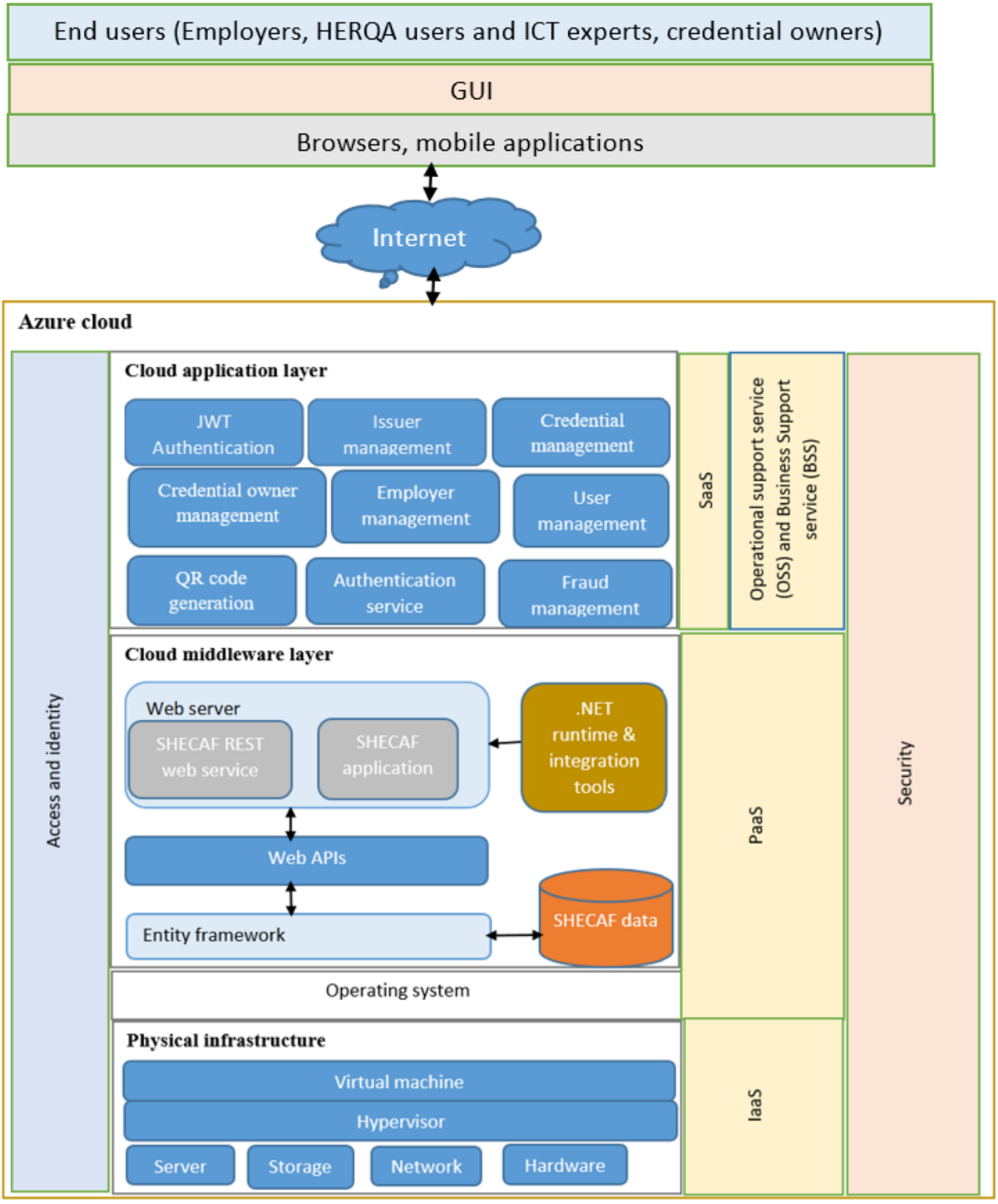


Figure 4. 6: Conceptual Framework of SHECAF

Figure 4.6 is own work, it consists of four layers managing the E-authentication components and the infrastructure for the provision of services. In the SHECAF, users / employers can request E-authentication services from the cloud provider. The details of the SHECAF layers are described below.

4.6.1 Users and End User Devices Layer

The device and user layer include

Users: - Employers, HERQA employees, and HEC holders with access rights and use of the system.

End-user devices: - End-users communicate with the cloud-based E-authentication system using browser-enabled devices such as handheld computers, laptops, desktops, tablets, and mobile phones using protocols such as SSH, http / https.

4.6.2 Presentation Layer

The presentation layer consists of components that implement and display the user interface and manage user interaction with the system. For E-authentication, the application graphical user interface, E-mail client, and web browser (including mobile devices) are used for user interaction with the system at the presentation level. User interface components provide a way for users to interact with the electronic authentication application. They render and format data for users, and they also collect and validate data entered by the user. In the presentation layer of the proposed system like: -

User Portal*:* - Provides the functions and features to authenticate and identify users and to provide a convenient, intuitive, personalized, and customizable web interface for facilitating access to information and services that are of primary importance and interest to users. In the E-authentication framework, it is an optional platform on which e-authentication components can be delivered.

4.6.3 Cloud Application Layer

Cloud application layer is the layer that is visible to the end-users of the cloud. Clients usually access the services provided by this layer through web-portals and APIs.

The main application services of e-authentication components from data analysis of the chapter 3 include:

JWT Authentication - is the service delivery, it is the secure log in and data transfer between end users and E-authentication system.

Issuer management**:** - As shown in Appendix A and B the interview and questionnaire respectively, a traditional way of authentication is dominant in the authentication of credentials and sources of credentials. However, it is inefficient, and there is a lack of transparency and person dependence processing. Therefore, we suggested an electronic credential issuing institutes that makes use of the cloud computing on the basis of digitally signed QR code and JWT technologies thereby implementing an instant messaging and notifications.

Credential management*:* - The proposed E-authentication system provides a proactive management information system for uploading, updating and authenticating verified higher education credentials.

Employer management: - Employer companies are registered and provided a user name and password for log in. employers can request authentication for employee credentials after logged in to the E-authentication system.

Credential owner management: - Credential owners can go to HERQA and request authentication for their credentials. When HERQA verifies the originality of the credentials, HERQA operator registers, updates and deletes the information of credential owners.

User management: - Different type of users can be added such as employer users, credential owner users, HERQA ICT users, HERQA data operators etc.

Fraud management: - The proposed E-authentication provides a workplace for reporting fraud uses for gaining job benefits.

QR code generation: - QR code is a two-dimensional bar code that can be read by smart phones and special devices. Our cloud based E-authentication generates a secure QR code that can be used by employers to request authenticity of education credentials of employees/candidates.

Authentication service: - This is the core reason component of the E-authentication system that can be consumed by mobile applications during scanning the QR code to retrieve original data of the credential from the central repository.

4.6.4 Operational Support Service

This service provides services such as provisioning, configuration, monitoring, service management, administration and logging through the use of web portals and APIs.

4.6.5 Business Support Service

Business Support service provides such as user management, authentication and authorization, security, contracts and agreements, reporting and analytic, customization, billing and metering.

4.6.6 Entity Framework

E-authentication units are used to transfer data between the E-authentication components. The data represents entities of the real electronic authentication, such as the QR code generator, the HERQA structuring, knowledgebase, Employer, Service, and the messaging service. The internal use of the electronic authentication application usually takes place. Alternatively, they can be implemented with custom object-oriented classes that represent the real entities in which the application should work.

4.6.7 Web API

The web API, as its name suggests, is an API on the web that accessed through the HTTP protocol. It is a concept and not a technology. We can build web API using different technologies like .NET, etc. It is an interface to communicate the user's HTTP request to the central service layer or the back-end implementation and the return HTTP response. So, we have chosen to use the web API because for the development of the prototype we have .Net Framework 6.0, it is compatible with the HTTP protocol, and we are familiar with ASP.NET, and MVC architecture.

In general, the web API used to communicate the HTTP request, the HTTP response data of the web application and the mobile application with the main services of the proposed system.

4.6.8 Cloud Middleware Layer

Cloud Middleware Layer provides a communication interface between the application and the operating system. It handles various operations by the client Middleware is highly essential in creating and publishing of business applications; encourages simultaneousness, transactions, threading and messaging; and provides a service component architecture framework for creating

service-oriented architecture (SOA) applications. Web servers, application servers and databases are cases of cloud middleware.

4.6.9 Cloud Service Delivery Components

The cloud service delivery components for the E-authentication include the followings:

***Software as a service*: -**SaaS layer is the second layer of the architecture below the presentation layer or user interface layer, which allows access to the hosted electronic office system and any third-party application software to run on the cloud platform. Services provided in the PaaS layer can be utilized by sending request messages through Web APIs. Therefore, the institution employers and users can access electronic authentication system and other third-party software through a web interface.

***Platform as a service*: -** PaaS layer is the third layer of the architecture, which is deployed on a cloud provider that can support a requirement of the designed platform. It consists two sub-layers called electronic authentication core service layer and service/data layer.

***Infrastructure as a service*: -** IaaS layer is the fourth layer of the architecture in which the cloud-based electronic authentication system is implemented. It contains the physical and virtualized infrastructure including the institution ICT Infrastructures.

4.6.10 Security, Access and Identity Management

Security is the ability of a system to prevent accidental actions outside its intended destination, which remains the big problem. Rightly, it allows access to resources and services based on assigned responsibilities. You should implement security and control at the process and data levels. Cloud computing has many security mechanisms to protect the data and the entire system holding and processing it. Outside of these mechanisms, the following are very common and are used in almost all cloud service providers. Also, for your own security methods [50]. The mechanisms are Firewall in hardware and software, Encryption, Hashing, Digital Signature, Public Key Infrastructure (PKI), Identity and Access Management (IAM), and Single Sign-On (SSO). In this study the IAM mechanism and Firewall was used.

IAM controls and tracks user identities and access privileges for electronic authentication, the knowledge-sharing environment. It includes components and policies such as authentication, authorization, user management, and credential management that are already provisioned for IaaS environment. In addition, remote management, resource management, SLA (Service Level

Agreement) management and billing management are used as a management mechanism in cloud computing.

These mechanisms typically provide unified APIs and can be offered as single results, custom applications, merged into different output sets or multi-function applications [51].

4.6.11 Conceptual System Architecture of SHECAF

The system architecture shows that the relationship among service requisition with request processing via internet. Before that the service delivery infrastructure must be prepared in order to perform the service requisition and service processing. Figure 4.7 below, shows the system architecture of SHECAF.

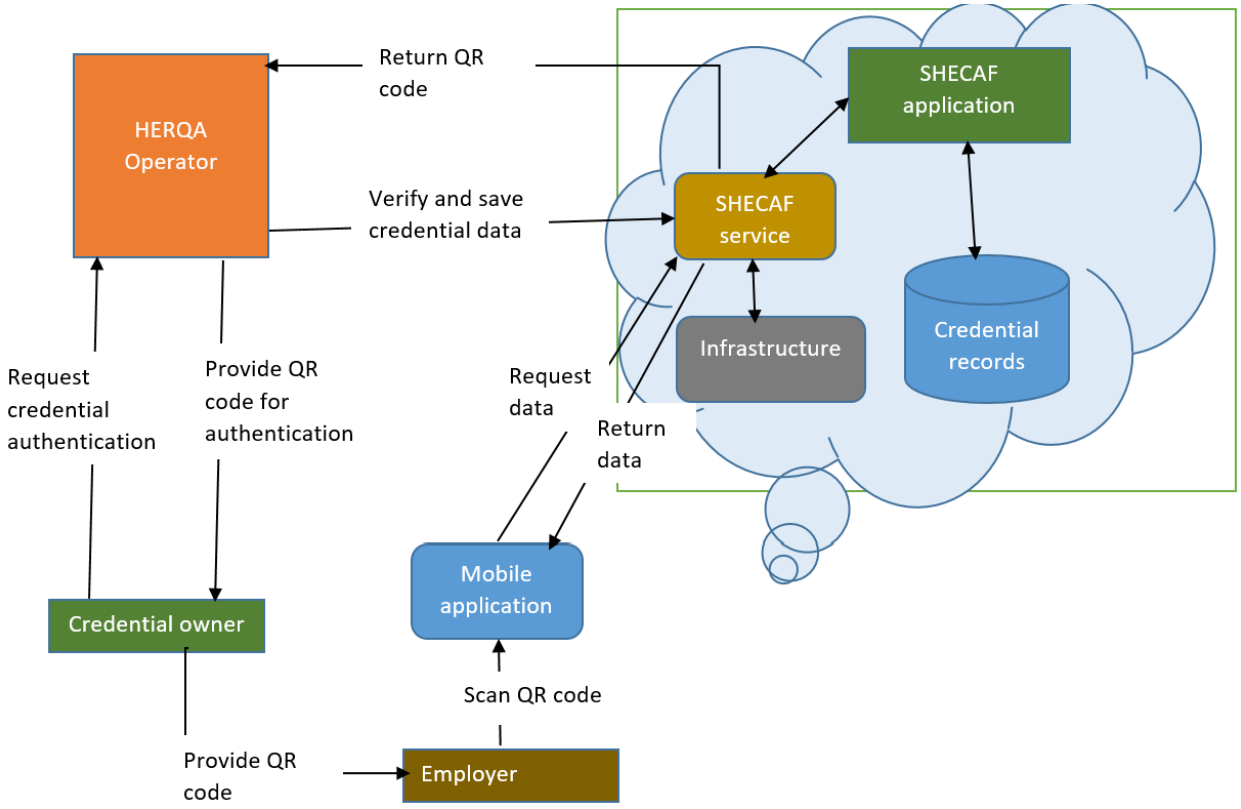


Figure 4. 7: SHECAF System Architecture

As depicted in figure 4.3 above the proposed E-authentication, SHECAF consists of five components the HERQA operator, Credential owner, Employer, Mobile application and the central repository for credentials.

Credential Owner:

Requests for authentication providing all the supportive information about his/her higher education credentials to HERQA operator.

HERQA Operator:

HERQA operator receives credential information from credential owner and uploads them to the database center after successfully verifying the credentials.

Database Center:

Generates a QR code for the stored credentials to be delivered to the credential for the purpose of later authentication by employers.

Employer:

Receives the QR code from job applicant or the credential owner and scan it to retrieve data from the database center for ensuring the authenticity of the credentials.

Mobile Application:

Used to scan the QR code on the credentials of the employee and send them to the database center through a REST web service.

Chapter Five: Prototype Building

5.1 Introduction

In this chapter, we provide an overview of the prototypical implementation of the proposed architecture, which was developed in chapter five. To this end, we focus on the implementation of some parts of the E-authentication system. This is the development of the front-end web application interface, an intelligent way to create a digital workplace; design services for uploading verified credentials, and manage services, generate QR codes and manage authentication of credentials. And web-based interfaces from Microsoft Azure providers of the system, the functionality of the link between each menu, the portability or the mobile device and tablet interface to search, and the desktop or laptop design of the developed prototype and other key functions to demonstrate the concept.

In this work, we apply the MVC mode, AJAX JS, Xamarin form, QR code algorithm, encryption algorithm, hashing algorithm, ADO.NET entity framework, Bootstrap, and other libraries used for the development of the user interface and ASP.Net for back-end implementation. Windows Azure cloud platform selected as application platform for implementation and creation, SQL server as a data storage in local and use SQL Azure database in Microsoft Azure.

5.2 Development Technologies

In the SHECAF, development environment for the cloud-based electronic authentication web application is configured; the employers, HERQA users and credential owners can access the system using different windows operating systems and web browsers. The UI of a cloud-based e-authentication system was created using AJAX, HTML, Xamarin forms and CSS for front or UI development and the editor used Jet Brains Web Storm 2016.3.1. Visual Studio IDE 2015 (ASP.net and MVC) architecture for backend or core service implementation and C # as the main language.

The integration of this SHECAF system with other systems of the mobile applications, university and national systems related to the proposed framework can be operated using JSON or other programming technology. For the purpose of managing and storing electronic authentication processes, transactions, and operations, we have used SQL Management Studio 2014, Azure storage service, and IIS8 is local server to deploy the application and it is other alternative of cloud deployment. The development platform is Window Azure platform (Platform as a Service).

5.3 The Proposed Framework Developed System Function

Based on the design architecture defined in the previous chapter, a demonstration web application was developed in the E-authentication web application to show how the framework and architecture can be used in the actual application.

The prototypical implementation of the proposed system: -

Firstly, credential owner goes to HERQA to request authentication for the issued higher education credentials.

Second, HERQA operator verifies the credentials and registers them into the proposed cloud storage. At this time the credential owner receives both the QR code and the log in credentials

Thirdly, Employer companies receive QR code from job applicants and scan it using mobile application to authenticate the originality of the documents presented by the candidates. The cloud storage returns the validity or invalidity of the documents.

Implement the prototype architecture and develop implementation details, interaction-oriented architectures as an architectural description concept. Every service can be identified by using code, and create based on service category to filter efficiently, effectively, and manage easily.

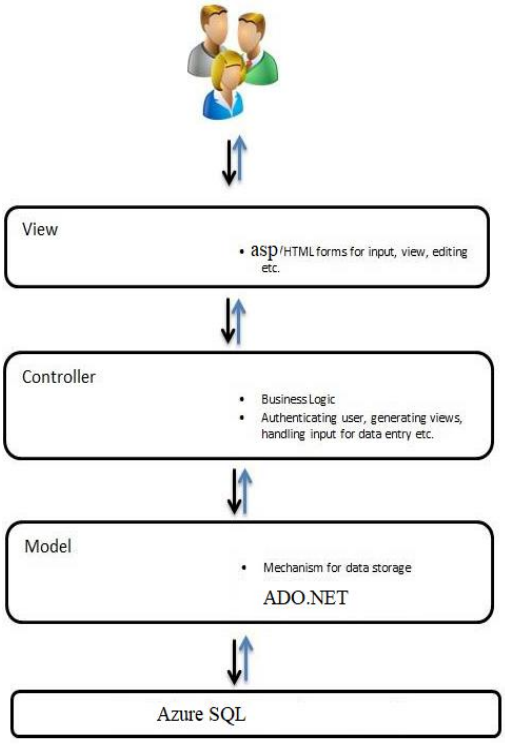


Figure Figure 5. 1: MVC architecture (adapted from [52]

Interaction-oriented software architecture consists of separating user interaction from data abstraction and processing business data, and splits the system into three main partitions. [52]:

- Data module / models: provides data abstraction, all business logic, or the core services of electronic authentication and interacts with the data layer.
- Controller module: respond to user action and direct the flow of the electronic authentication.
- View module: it is responsible for the visual presentation of the data output, it also provides an interface for the user input. Format and present the data from the model to a user.

In general, Figure 5.1 above shows that the MVC architecture to the view of user interaction up to data layers from each user interface. When the user clicks an action, by creating AJAX JS module, then forwards/routing path, and create global variable to store service data, call the config base paths, the controller creates and uses objects, communicate with service / factory then connect to HTTP interceptor in order to communicate with WebAPI through the URL, core services, and data layer. All communication is done in two ways. Then data is send request and return response.

5.4 DataBase Design

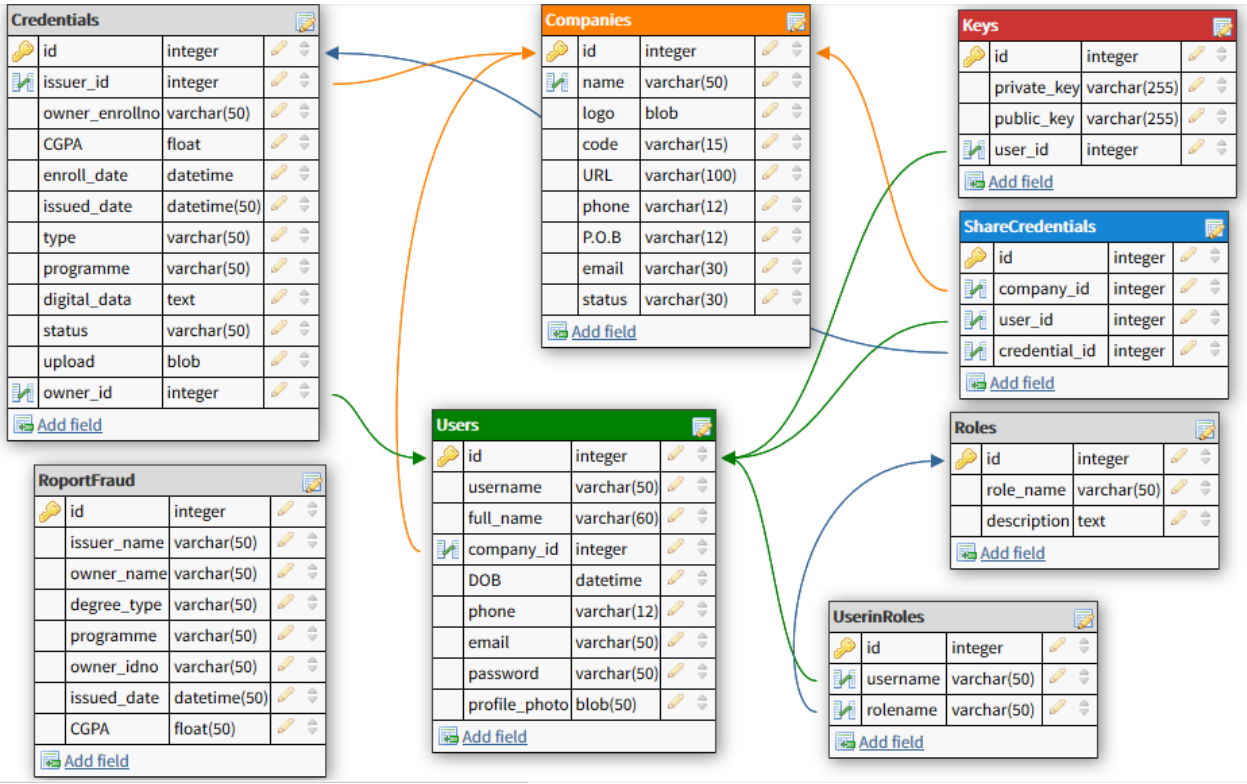


Figure 5. 2: Database Design

We have implemented an E-authentication database in the scalable cloud database Azure SQL. Figure 5.2 provides an overview of this database. The tables used in our implementation are:

- The **companies** table contains basic higher education or employer information. The **Keys** table saves the public and private key pair, which is used for creating the digital signatures. The public and private key pair is generated when an individual user is registered in our system. The user_id in this table is the foreign key from the **Users** table.
- The Role table saves every identified role in every identified users.
- When a QR code ciphertext is created by using a hash algorithm and the private key of the user (the credential owner), a digitally signed data is saved in the **Credentials** table and a user can share it for authentication to employers and other organs that needs to know the originality of the credentials that the owner claims as a proof of qualification and competency. When the user shares credentials for various purposes the user id, organization id and credential id are saved in the **ShareCredentials** table to serve as access

right is granted by the owner of the credentials. This way, the scanner gets the entire authorized user identifiers associated with a specific code with a single query.

- **ReportFraud** table is used to store illegitimate attempts to gain job benefits by creating a counterfeited educational credentials.

5.5 User Interface

This section shows the overview of the presentation layer that interacts with the users. The proposed E-authentication application two applications the mobile application and web application. Both needs user to log in to access the authentication system. The mobile application is mainly used to scan QR codes to request authentication of credentials from the cloud based database of higher education credentials. However, the web application is the application that HERQA manages for registering issuing institutes, employers and credential owners along with their credentials to provide authentic data about employees' higher education credentials.

Figure 5. 3: Log in and Scan Interface from Mobile Application

Figure 5. 4: Authentication Result

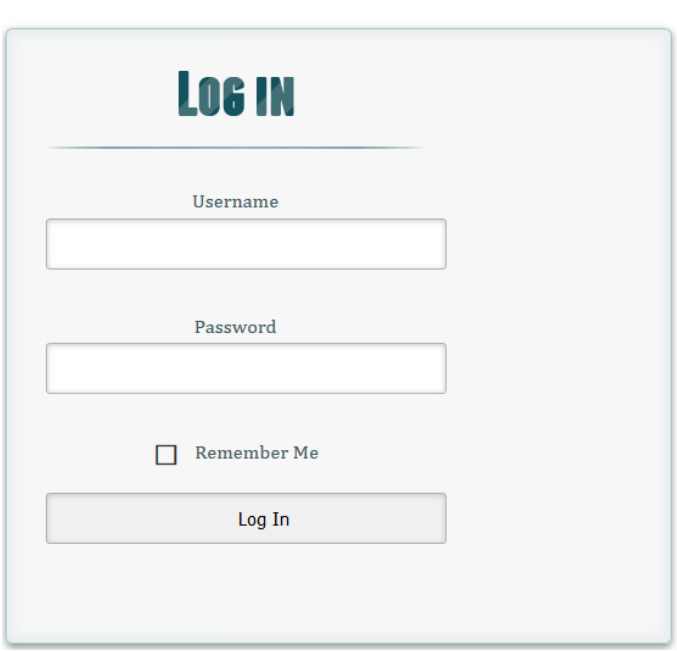


Figure 5. 5: Log in Page for the Web Application

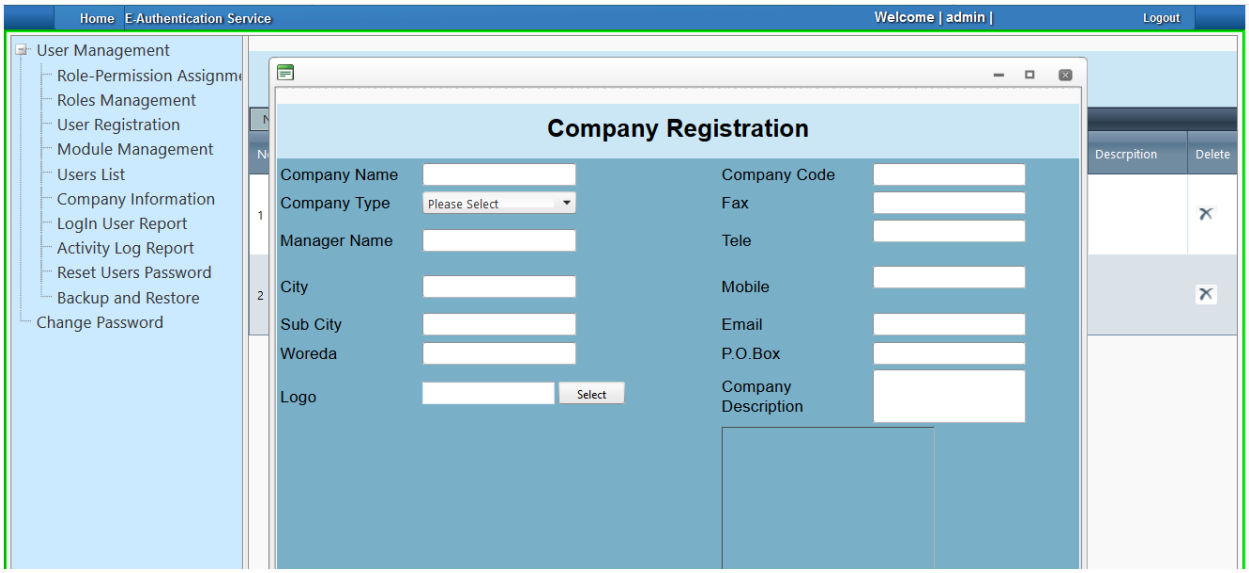


Figure 5. 6: Company Registration Page

5.6 Implementation Environment

5.6.1. Mobile Application

We developed a cross platform application that can run on android, apple operating system, mac operating system, and windows operating system. The code was written using the .NET xamarin forms. The application was compiled and tested using various software development kits and android device. JSON was used as a web service that provides the interface between the mobile application and the cloud database.

5.6.2. Web Application

The web application was developed using the .NET framework based on ASP.NET and ADO.NET framework. The application and web service was hosted on the azure cloud internet information security (IIS) server.

5.6.3. Database

The database was developed using the azure SQL database. SQL database is very compatible with ASP.NET and other platforms. Furthermore, it is simple and secure database management system which is widely used by Microsoft applications and platforms.

5.7 Implementation Details

5.7.1. JWT Authentication

JSON web token (JWT) was used to exchange services, and resources between the web application and the application securely. JWT uses digital signature to ensure a secure transmission of information between parties. JWT consists of three parties, header, payload and signature separated by dot. The header represents the type of the token and the encryption algorithm whereas the payload contains the claims. Finally we have the signature part which is the digital token formed by the header, payload and secret key and the web application server uses it to verify whether the token has valid information or not.

Figure 5. 7: JWT Authentication

5.7.2. QR Code Generation

A unique digitally signed QR code is generated upon a credential owner request using the E-authentication service. The digital data is used as a unique identifier of the credentials of an individual. The procedures for generating the QR code includes:

- Registration of verified credentials
- Providing a log in credential for credential owners
- Credential owner log in and request QR code
- QR code is generated based on a digitally signed predetermined credential information
- Credential owner can share this QR code with third party such employers and recruiting agencies.
- The third party can scan the QR code using a mobile application to get a verified data of individual credentials

Chapter Six: Evaluation, Result and Discussion of the Study

In this section, we review surveys that we conducted with users, IT professionals, and software development experts to evaluate and discuss the prototype system being developed and discuss the current manual system. The current practice of processing HERQA authentication tasks is through a manual method. There are many problems with the current manual method, such as: delays in responding authentications to employer companies and authentication seeker individuals, inconsistency with office work procedures, and reviews, time spent on non-core tasks, lack of coordination / communication, delays in decision-making due to time spent in retrieving facts and information, lack of security and confidentiality of credentials, and unavailability of responsible officers.

Reflect on the previous problems, we have proposed a platform framework based on the cloud (Software as a Service) and implemented a prototype system that creates a common alliance through the use of manual method to electronic authentication work, then bringing institutional and individual efficiency through faster decision-making, error free output, collaborative workspaces, communication speed, optimal resource utilization, scalability, and movement effectiveness through output / result orientation, quality of output, on-time delivery, and cost effectiveness (value for money) through accessibility and availability of information and through commitment. Transparency is created to provide employers with user-friendly operation, a trusted digital environment, easy file retrieval, remote capabilities, and online help / assistance.

Compared to the manual method, it follows the standard workflow and services fraud reporting, logging of transaction history, interactive and supported by current technologies and tools, but does not mean that it replaces the entire manual authentication process, but as a bridge for software developers.

ICT professionals from HERQA, employer companies, and experts in software engineering, related fields evaluated the design of the technical system give their comments and suggestions on the SHECAF system developed. They recommend that the system more users friendly and easier to use to be more effective. Therefore, the comments were positive and these comments and recommendations were left to the respective HERQ to the professionals who perform their functions, and the development of the full implementation will be easy for the software engineers.

Finally, this architecture and framework for sharing higher education credentials and simple communication between employers has been found through the implementation of mobile application, REST web services, digitally signed QR codes and JWT authentication and building of an exchange institutional knowledge is effective and important if it is fully implemented with the comments of all interested stakeholders.

To validate this evaluation was done on how users use the SHECAF UI and attractive interface. They practiced/used the designed user interface and other features of the developed prototype. Finally, they suggest several additional problems to be included in the system. Therefore, the evaluation questions were made with four (4) HERQA employers from different offices, three (3) ICT professionals working in the HERQA, three (3) experts and eight (8) colleagues in software engineering and related fields. In general, total of twenty (20) respondents participated in the evaluating the developed prototype.

To evaluate the SHECAF system, each user group uses its own pages created for them. Moreover, rate the result in terms of usability of the prototype and framework of the SHECAF system in the cloud. The framework and developed prototype evaluate and re-work the framework and modify the prototype.

Here is the evaluation result prepared from the prototype-developed system and framework of the SHECAF system. It represents Poor (1), Fair (2), Good (3), V. Good (4), Excellent (5).

Table 6. 1: Evaluation criteria for developed prototype system and framework of the SHECAF

No	***Evaluation Criteria***	***1***	***2***	***3***	***4***	***5***
1	How do you rank your satisfaction with the developed prototype system?	-	2	10	5	1
2	How do you rank the use of a mobile application readable secure QR code for the authentication of higher education credentials?	-	-	9	7	2
3	How do you rate the response time of the developed prototype?	-	1	9	8	-

Evaluation Criteria's (Question 4-8, Answered by Expert in Software Engineering and Related Field)						
No	***Evaluation Criteria***	***1***	***2***	***3***	***4***	***5***
4	How do you rate the problem of non-standard process solutions in the design framework and in the developed prototype system?	-	-	8	6	4
5	How do you evaluate the framework and prototype that was developed to solve the challenges of the manual authentication of higher education credentials?	-	2	7	6	3
6	How do you rank the prototype-developed system to decrease the time lost in non-core process?	-	2	9	6	1
7	How do you rate the security and integrity features of the proposed framework and prototype for authenticating higher education credentials?	-	1	4	10	3
8	How do you evaluate the selection of deployment service for the E-authentication service being a private cloud?	-	2	5	9	2

As a user of the SHECAF system in Table 6.1: shows a summary result of the evaluation for developed prototype system.

First criteria, is the satisfaction of the evaluator of the prototype-developed system rated as fair, good, very good, and excellent by 11%, 27.7%, 38.8%, and 22.2% of the respondents respectively. As we have seen from the result of the evaluation the developed prototype, most of the evaluator give their satisfaction good and very good. Moreover, most of the evaluator have a good perspective for the prototype-developed system.

Second criteria, the rating of using the machine readable secure QR code is good, very good, and excellent by 27.7%, 38.8%, and 33.3% of the respondents respectively. As we have seen from the response most of the respondent responded V. Good and excellent about the dynamic form builder.

Third criteria, the browser response time starting to request a service on the server be rated as fair, good, very good and excellent by 5.5%, 50%, 33.3% and 5.5% of the respondents respectively.

Fourth criteria, the problem of non-standard process solutions in the design framework and developed prototype system rated as good, very good and excellent by 38.8%, 44.4%, and 16.6% of the respondents respectively.

Fifth criteria, the design framework and the developed prototype system for solving the challenges of manual authentication is rated as fair, good, very good and excellent by 16.6%, 33.3%, 38.8%, and 11% of the respondents respectively.

Sixth criteria, the prototype developed system to decrease the time lost in the non-core process is rated as fair, good, very good and excellent by 5.5%, 27.7%, 55%, and 16.6% of the respondents respectively.

Seventh criteria, the security and integrity of credentials in the proposed electronic authentication system is fair, good, very good, and excellent by 5.5%, 38.8%, 44.4%, and 16.6% of the respondents respectively. This shows that the responders are confident enough that our proposed collaborative, secure and reliable system will bring security and integrity thereby rooting out the use of fake credentials for job benefits.

Eighth criteria, the private cloud deployment model for securing the authentication process and records of at the central repository is rated as fair, good, very good and excellent by 11%, 27.7%, 55.5%, and 5.5% of the respondents respectively.

In general, as we have shown in the previous discussion on the most evaluative response, when the cloud-based electronic authentication implemented increases effectiveness, transparency of authentication tasks, decreases the time lost in non-core processes and facilitates the work of the institution, the use of mobile readable secure QR code also responded that it is a good and very good idea to solve the problems of the enormous manual way of authentication and to have an automatic authentication and management of credentials in the agency. In addition, the design framework has an automatic distribution of tasks and an escalation engine to complain to a higher level of management and to create a faster interaction and collaboration.

Chapter Seven: Conclusion and Future Work

7.1 Conclusion

In Ethiopia, employer organizations are ending up hiring unqualified employees due to the increased use of fraud higher education credentials to obtain job benefits. HERQA and Higher education institutes have not any adequate technique that provides a fast and fraud detecting verification and authentication. Therefore, we have taken HERQA to solve related to the problems regarding to verification and authentication of higher education credentials. To solve the problems, we propose the cloud-based electronic authentication framework and prototype implementation for the HERQA. In this study, we introduced the private cloud platform architecture and prototype implementation of electronic authentication called SHECAF for verifying and authenticating higher education credentials from employer organizations, collaboration and messaging, and escalation engines to have alerts and notifications, SMS and E-mail exchange, to have fraud reporting platforms and managing institutional knowledgebase. Therefore, this study introduces the concept of implementing cloud computing into verification and authentication of higher education credentials to eliminate the use of forged credentials and manual verifications which is time consuming and labor intensive. SHECAF is based on IBM, NIST Cloud Reference Architecture, and Microsoft Web Application Architecture. We have developed a cloud-based framework of electronic verification and authentication for HERQA. For the designed architecture, a prototype system was developed and hosted on the Microsoft Azure platform.

This NIST architecture focused on electronic verification and authentication services to increase availability at a low cost and to create a good communication and collaboration network. Various users, ICT professionals, other experts, and colleagues in software engineering and related fields evaluate the developed prototype web application. The proposed framework is just the roadmap for implementing an entire electronic authentication and service delivery ecosystem. It facilitates and creates a digital workplace solution and an intelligent environment. Furthermore, this study contributes to future related studies on the application of cloud computing and Secure QR code to ensure the integrity and security of higher education credentials.

7.2 Future Work

The proposed framework is not the complete system developed, but we prepare the prototype.

The proposed system was developed for HERQA. The presented architecture and the prototype implemented in this thesis must be improved and evaluated for a more complete and worthy electronic authentication task. Furthermore, even if the integration of this SHECAF system with the signature tool was shown in the proposed framework and architecture, this feature is not implemented in the prototype. When HERQA implements the cloud based electronic authentication framework we recommend a private cloud deployment model due to the sensitivity of the data for educational documents.

In addition, there are different components or functionalities of E-authentication not implemented such as: alerts and notifications to notify clients for different status, develop electronic messaging and collaboration, escalation and dispatcher engines, SMS and Email exchange.

Here is a list of some of the future work such as:

- A systematic study on other technologies for preventing paper based documents and conduct a thorough comparison and analysis to identify the best and more effective verification and authentication mechanism regarding to employee educational documents.
- A fully automated intelligent system that supports both offline and online full automatic verification and authentication can be developed.

References

[1] W. Tamrat, "Academic credential fraud – In search of lasting solutions," *University World News*, 2017. [Online]. Available: https://www.universityworldnews.com/post.php?story=20171214061717655. [Accessed: 23-May-2019].

[2] Z. Yahya *et al.*, "A New Academic Certificate Authentication Using Leading Edge Technology," in *Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government*, 2017, pp. 82–85.

[3] O. Ghazali and O. S. Saleh, "CLOUD BASED GRADUATION CERTIFICATE VERIFICATION," p. 5, 2016.

[4] A. Singhal and R. S. Pavithr, “Degree Certificate Authentication using QR Code and Smartphone,” *Int. J. Comput. Appl.*, vol. 120, no. 16, 2015.

[5] N. M. Musee, “An academic certification verification system based on cloud computing environment,” *PhD Diss Univ. Nairobi*, 2015.

[6] “HERQA takesmeasures on 15 colleges, campuses | The Reporter Ethiopia English.” [Online]. Available: http://www.thereporterethiopia.com/article/herqa-takesmeasures-15-colleges-campuses. [Accessed: 23-May-2019].

[7] A. Negussie, “Ethiopia: Fake Documents Rob Nation in Daylight,” *Addis Fortune (Addis Ababa)*, 20-Feb-2018.

[8] “Ethiopia launches investigations on private colleges – New Business Ethiopia,” 2019. .

[9] “MoE partners INSA to root out employees with fake documents | The Reporter Ethiopia English.” [Online]. Available: https://www.thereporterethiopia.com/article/moe-partners-insa-root-out-employees-fake-documents. [Accessed: 08-Sep-2018].

[10] H. Pandit, S. Nipane, S. Jadhav, and S. Naik, “Secured E-Documents and Sharing using Encrypted QR-Code.”

[11] “Gambella fires nine senior officials for fake documents | The Reporter Ethiopia English.” [Online]. Available: https://www.thereporterethiopia.com/content/news-brief-32. [Accessed: 08-Sep-2018].

[12] L. du Plessis, N. Vermeulen, J. van der Walt, and L. Maekela, “Verification of Qualifications in Africa,” 2015.

[13] R. M. Kaibiru and B. Shibwabo, “A Prototype for authentication of secondary school certificates: a case of Kenya certificate of secondary education,” 2017.

[14] E.-A. Adán, “The Forensics of Academic Credential Fraud Analysis and Detection,” p. 13.

[15] M. I. Malkawi, “Counterfeit Prevention and Detection of University and Academic Institutions Documents Using Unique Codes,” US20170352039A1, 07-Dec-2017.

[16] Y. A.C, R. H.R, A. Punith G.B, and Rajesh.B, “A design and development of a model to authorize certificates in government sectors using cloud computing technology,” *Int. J. Adv. Technol. Eng. Res.*, vol. 2, no. 2, 2012.

[17] K. H. Pandya and H. J. Galiyawala, “A Survey on QR Codes: in context of Research and Application,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 4, no. 3, pp. 258–262, 2014.

[18] E. Gorelik, “Cloud Computing Models,” Massachusetts Institute of Technology, 2013.

[19] P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.

[20] N. Y. Chong, “Cloud Computing Challenges in a General Perspective,” . *Volume*, vol. 3, no. 1, p. 15, 2019.

[21] S. Carlin and K. Curran, “Cloud Computing Technologies,” *Int. J. Cloud Comput. Serv. Sci. IJ-CLOSER*, vol. 1, no. 2, Jun. 2012.

[22] T. Walters, “261-2009: SAS® as SaaS: The Benefits and Challenges of Implementing an Enterprise-Scale SAS Data Warehouse and Business Intelligence Shared Service,” p. 9, 2009.

[23] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, “NIST Cloud Computing Reference Architecture,” in *2011 IEEE World Congress on Services*, Washington, DC, USA, 2011, pp. 594–596.

[24] S. Saidhbi, “A cloud computing framework for Ethiopian Higher Education Institutions,” *IOSR J. Comput. Eng.*, vol. 6, no. 6, pp. 01–09, 2012.

[25] V. H. Pardeshi, “Cloud computing for higher education institutes: architecture, strategy and recommendations for effective adaptation,” *Procedia Econ. Finance*, vol. 11, pp. 589–599, 2014.

[26] M. Hamdaqa and L. Tahvildari, “Cloud computing uncovered: a research landscape,” in *Advances in Computers*, vol. 86, Elsevier, 2012, pp. 41–85.

[27] M. F. Erkoç and S. B. Kert, “Cloud computing for distributed university campus: A prototype suggestion,” in *International Conference on Future of Education, Firenze*, 2011.

[28] Department of Computer Engineering, Anantrao Pawar College of Engineering and Research, Pune, Maharashtra, India *et al.*, “Develop the Cloud Based Personal Document Storage System and Retrieve Them Using QR Code,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 4, pp. 312–314, Apr. 2017.

[29] M. Endris, “Participatory Indigenous Knowledge Management Architecture for Traditional Medicine,” *Adama Sci. Technol. Univ.*, 2016.

[30] D. Howitt, *Introduction to qualitative methods in psichology*. México: Pearson Educación, 2011.

[31] O. Bentahar and R. Cameron, “Design and Implementation of a Mixed Method Research Study in Project Management.,” Jan. 2015.

[32] J. Pansiri and U. D. Jogulu, “Mixed methods: a research design for management doctoral dissertations,” *Manag. Res. Rev.*, vol. 34, no. 6, pp. 687–701, May 2011.

[33] D. Fallman, “Why research-oriented design isn’t design-oriented research,” *Nordes*, no. 1, 2005.

[34] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” p. 33.

[35] M. Mattsson, H. Grahn, and F. Mårtensson, “Software Architecture Evaluation Methods for Performance, Maintainability, Testability, and Portability,” p. 10.

[36] D. Bell, *Software engineering for students: a programming approach*. Pearson Education, 2005.

[37] M. B. Wall, K. T. Ulrich, and W. C. Flowers, “Evaluating prototyping technologies for product design,” *Res. Eng. Des.*, vol. 3, no. 3, pp. 163–177, 1992.

[38] W. Tamrat, “Academic credential fraud – In search of lasting solutions,” 2017. [Online]. Available: www.universityworldnews.com/article.php.

[39] M. Q. Patton, *Qualitative evaluation and research methods*. SAGE Publications, inc, 1990.

[40] J. Mäenpää, “Cloud computing with the Azure platform,” in *TKK T-110.5190 Seminar on Internet Working*, 2009.

[41] D. Sullivan, “PaaS Providers List: 2014 Comparison And Guide,” *Tom’s IT January 31 2014 Addit. Available Httpwww Tomsitpro Comarticlespaas-Provid.*, pp. 1–1517, 2014.

[42] “Amazon Web servives,” *Amazon Web servives*, 21-Dec-2019. [Online]. Available: aws.amazon.com.

[43] A. Zahariev, “Google app engine,” *Hels. Univ. Technol.*, pp. 1–5, 2009.

[44] “Microsoft Visual Studio,” *Wikipedia*. 24-Apr-2019.

[45] “All About Visual Studio .Net.” [Online]. Available: https://www.c-sharpcorner.com/blogs/all-about-visual-studio-net1. [Accessed: 03-May-2019].

[46] *IBM Cloud Computing Reference Architecture (CCRA) 4.0 Overview*. IBM, 2014.

[47] “NIST cloud reference architecture.”

[48] Microsoft Corporation, “Web Application Architecture Guide.” Microsoft Corporation, 2008.

[49] M. Keeling, “Dealing with Constraints in Software Architecture Design,” 22-Oct-2014. .

[50] M. Sajjad Ali, “Cloud Management Mechanisms,” 09-Oct-2014.

[51] M. Sajjad Ali, “Cloud Security Mechanisms,” 09-Oct-2014.

[52] “Software Architecture and Design.” [Online]. Available: Available: https://www.tutorialspoint.com/software_architecture_design/interaction_oriented_architecture.htm. [Accessed: 04-May-2019].

Appendixes

Appendix A: Interview Questions

Interview: director of the higher education permit issuance, accreditation issuance, and credential authentication issuance deputy director general and the three directors under him and the ICT director as well should respond questions.

1. How is the higher education credentials Authentication process handled?
2. What is involved in the authentication process?
3. What are the requirements for higher education credentials to get authenticated?
4. How do you rate the efficiency and effectiveness of the current authentication regarding to the security and integrity of higher education credentials?
5. What are the challenges of the current authentication approaches?
6. How long does it take to respond for an authentication request?
7. How do you track the status of an authentication request at different levels of the organization structure?
8. How responsible are the officers to be accessible during the authentication request?
9. Is there any plan to enhance the security and integrity of higher education credentials?
10. If your agency have a tendency to adopt a paperless system for the authentication of higher education credentials which approach do you suggest? Traditional computing approach or Cloud computing approach?
11. What can be the possible reasons to select the cloud computing technology?
12. Does your agency have all the required resources and competency to build an efficient, secure, reliable and collaborative database of higher education institutes and their credentials at a national level?

Appendix B: Questionnaire Questions

Higher Education Credentials Authentication Questionnaire Questions

The purpose of this self-administered questionnaire is to investigate and gather information on the process of authenticating higher education credentials and your agency's competency and tendency to adopt a secure, reliable, fast and convenient digital system to weed out the use of fake credentials across the country. Therefore, I would like to request you to fill this questionnaire carefully. The information that you provide me through the questionnaire would be highly important to the research we are undertaking.

All responses that you provide will be treated confidentially and only for academic purposes.

1. How do you verify HE credentials*?*

   ☐ Manual verification

   ☐ HE database

   ☐ National database

   If any other use specify here ….....

2. How long does it take to verify/authenticate HE credentials in days?

   ☐ Two days

   ☐ Seven days

   ☐ Ten days

   ☐ Fifteen days

   If any other specify----------

3. What criterion do you use to verify/authenticate HE credentials?

   ☐ Issuer name

   ☐ Issuer logo

   ☐ Issuer seal

   ☐ Issuer signature

   ☐ Holder name

   ☐ Holder ID

- ☐ Holder registration number
- ☐ Holder age
- ☐ Degree type
- ☐ Faculty name
- ☐ Department name
- ☐ Course taken
- ☐ course grade
- ☐ CGPA
- ☐ Entry date
- ☐ Issued date

If other, specify----------

4. Does your agency has a common standard and framework for the authentication of higher education credentials?
   - ☐ Yes
   - ☐ No

5. Is there any sound mechanism to trace the status of authentication progress?
   - ☐ Yes
   - ☐ No

6. Does the current authentication method has any easy way to locate authenticated credentials?
   - ☐ Yes
   - ☐ No

7. Have you ever had cases where HE credentials were lost during searching for authentication?
   - ☐ Never
   - ☐ Not so often
   - ☐ Most of the time

☐ Always

8. Have you ever had any cases of faked HE credentials? (**Select only one**.)

☐ Never

☐ Not so often

☐ Most of the time

☐ Always

9. Is there any platform to report/inform fraud cases from various stakeholders?

☐ Yes

☐ No

10. What are the challenges faced by the current authentication way of HE credentials?

☐ Time consuming

☐ Costly

☐ Unavailability of responsible officer

☐ Susceptible to fraud

☐ Other

If other, please specify_____

11. What would be the effects of using fake HE credentials to gain employment benefits?

☐ Socio-economic failure

☐ Escalation of other illegal practices and corruption

☐ Lack of trust and declined quality of education

☐ Damage of reputation and income

☐ Other (**please list them below**)

---

12. What is your level of satisfaction in regard to the efficiency and effectiveness of the current authentication method?

- ☐ Extremely high
- ☐ High
- ☐ Very high
- ☐ Low

13. Do you think the implementation of E-authentication system in your agency will enhance the security and integrity of credentials and the efficiency and effectiveness of the authentication task?

- ☐ Yes
- ☐ No

14. Do you recommend the adoption of cloud computing technology for the implementation of an E-authentication application?

- ☐ Yes
- ☐ No

Appendix C: Observation on Services

Observation checklists:

- How does a higher education credential get authenticated and what are the interactions involved to verify it
- Requirements for credential authentication
- An insight on the time an authentication of a credential can take
- Current technique of authentication
- Challenges of the authentication process

Appendix D: Evaluation Criteria Questions

Here are the evaluation criteria prepared from the prototype-developed system and design framework of SHECAF. It represents Poor (1), Fair (2), Good (3), Very Good (4), Excellent (5).

Evaluation Criteria (Question 1-3, Answered by HERQA users and ICT professionals)

1. How do you rank your satisfaction with the developed prototype system?
   A. Fair B. Good C. Very Good D. Excellent
2. How do you rank the use of a mobile application readable secure QR code for the authentication of higher education credentials?
   A. Fair B. Good C. Very Good D. Excellent
3. How do you rate the response time of the developed prototype?
   A. Fair B. Good C. Very Good D. Excellent

Evaluation Criteria (Question 4-8, Answered by Expert in Software Engineering and Related Field)

4. How do you rate the problem of non-standard process solutions in the design framework and in the developed prototype system?
   A. Fair B. Good C. Very Good D. Excellent
5. How do you evaluate the framework and prototype that was developed to solve the manual authentication of higher education credentials?
   A. Fair B. Good C. Very Good D. Excellent
6. How do you rank the prototype-developed system to decrease the time lost in non-core process?
   A. Fair B. Good C. Very Good D. Excellent
7. How do you rate the security and integrity features of the proposed framework and prototype for authenticating higher education credentials?
   A. Fair B. Good C. Very Good D. Excellent
8. How do you evaluate the selection of deployment service for the E-authentication service being a private cloud?
   A. Fair B. Good C. Very Good D. Excellent

Appendix E: Working with Microsoft Window Azure Platform

In this section, we discussed how to work with Microsoft window azure to develop and host application. So, to create the proposed application on window azure platform services: we have used App service; that is the platform services is provided to the user by app service. The APP services enable developers to focus on their code and reach a stable, highly scalable production state quickly. With APP services, we can develop the web app, mobile app, API APP, logic API etc. Among this, we have selected the web app services.

To create the web app services on the Azure app service platform, we have followed the following three steps.

1. Selecting app service type

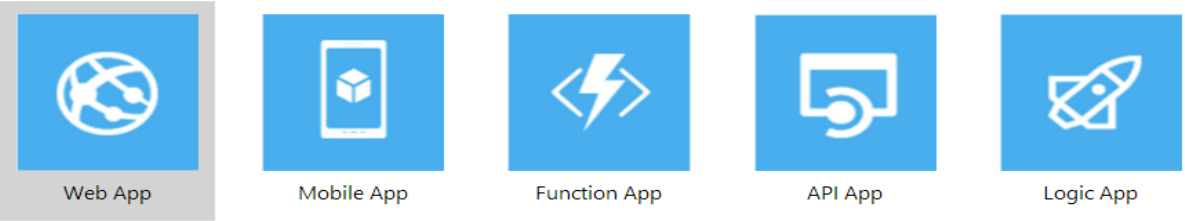


Figure 1: Web App Service Type

As we shown in above figure, we have selected web app service. Azure Web Apps enable developers to easily deploy and scale enterprise grade web applications written in a variety of languages and integrated with a multitude of services without ever worrying about infrastructure management.

2. Selecting a language in window azure platform, there is Visual Studio integration tools that allows for the developer for creating, deploying, and debugging applications in online and at developer local machine. The following diagram shows the language selected and its template.

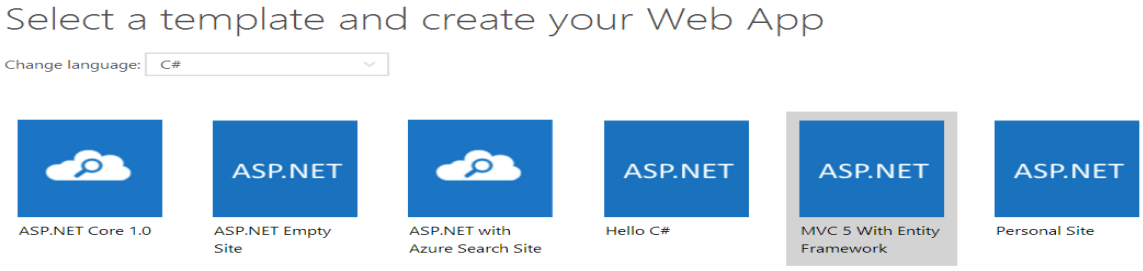


Figure 2 : Selection of Language in Window Azure Platform

3. Creating the web app services and other related information to deploy the application.

Appendix F: Sample User Interface

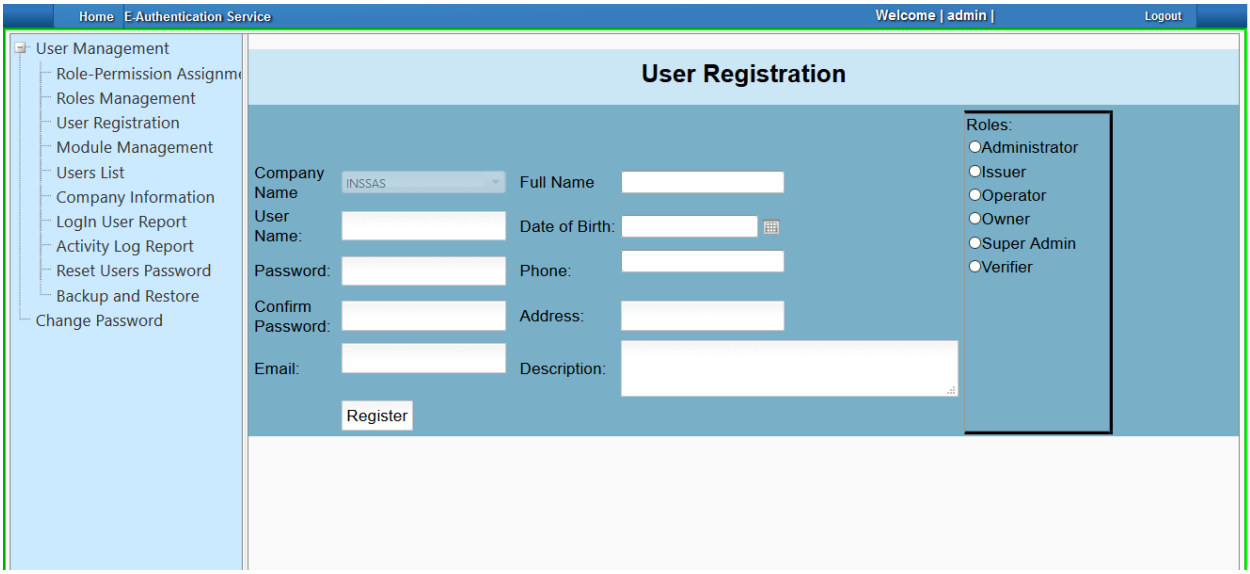


Figure 3: User Registration Form

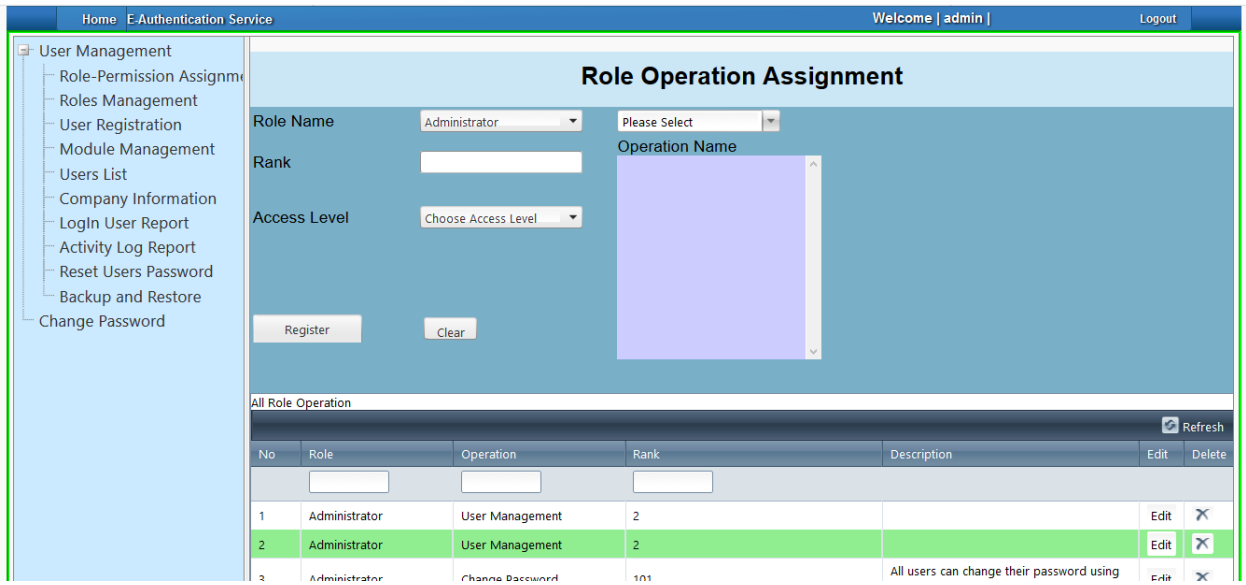


Figure 4: Role Operation Assignment

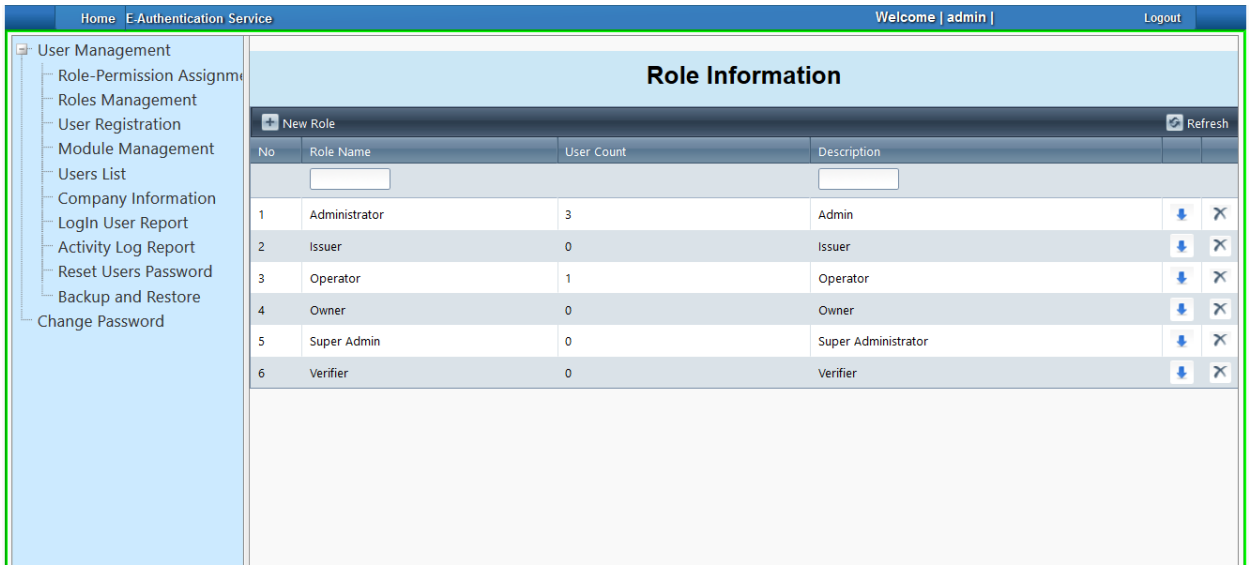


Figure 5: Role Management

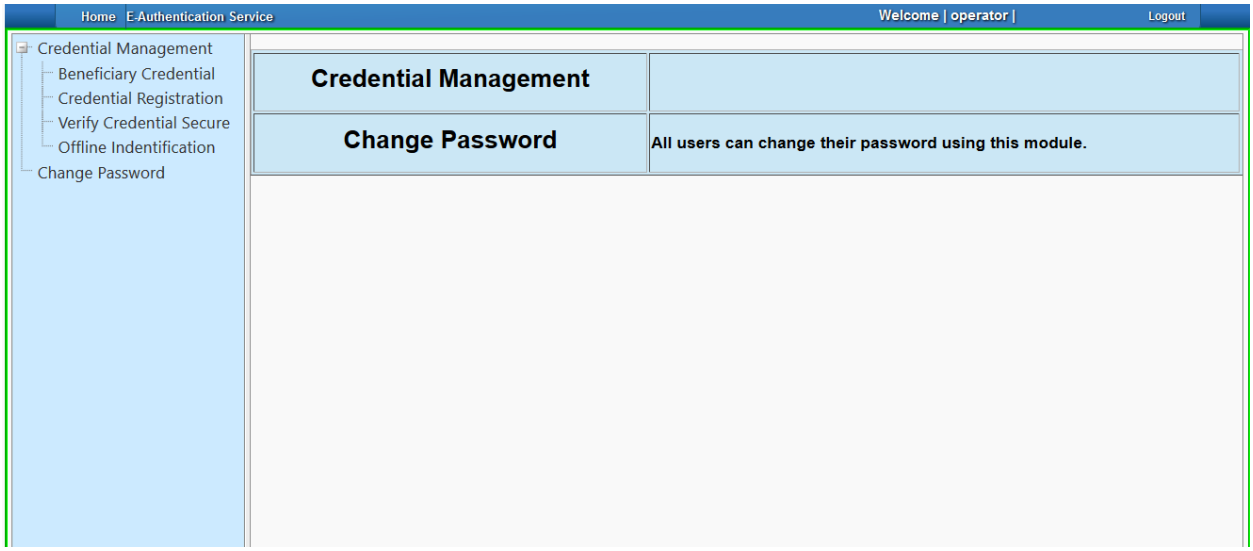


Figure 6: Credential Management

Appendix G: QR Code Generator Code

```
//ZXING LIBRARY REFERENCE
using com.google.zxing.qrcode;
using com.google.zxing.common;
using com.google.zxing.qrcode.decoder;
using SecureQRCode;

namespace SecureQRCodeWeb

{
   public partial class QRCodeGenerator : System.Web.UI.Page
  QRCodeWriter writer = new QRCodeWriter();
        Hashtable hints = new Hashtable();

        hints.Add(com.google.zxing.EncodeHintType.ERROR_CORRECTION,
errorCorrectionLevel);
        hints.Add("Version", version);
        hints.Add("Mode", mode);
        hints.Add(com.google.zxing.EncodeHintType.CHARACTER_SET, "utf-8");
        ByteMatrix byteIMGNew = writer.encode(txt,
com.google.zxing.BarcodeFormat.QR_CODE, 400, 400, hints);
        sbyte[][] imgNew = byteIMGNew.Array;
        Bitmap bmp1 = new Bitmap(byteIMGNew.Width, byteIMGNew.Height);
        Graphics g1 = Graphics.FromImage(bmp1);
        g1.Clear(Color.White);
        for (int i = 0; i <= imgNew.Length - 1; i++)
        {
           for (int j = 0; j <= imgNew[i].Length - 1; j++)
           {
              if (imgNew[j][i] == 0)
              {
                 g1.FillRectangle(foreColor, i, j, scale, scale);
              }
              else
              {
                 g1.FillRectangle(backColor, i, j, scale, scale);
              }
           }
        }

        bmp1.Save(Server.MapPath("~/Images/QR_Codes/" + "img.jpg"),
System.Drawing.Imaging.ImageFormat.Jpeg);
        bmp1.Save(Server.MapPath("~/Images/QR_Codes/" + "img.png"),
System.Drawing.Imaging.ImageFormat.Png);
```

```
        bmp1.Save(Server.MapPath("~/Images/QR_Codes/" + "img.gif"),
System.Drawing.Imaging.ImageFormat.Gif);
        bmp1.Save(Server.MapPath("~/Images/QR_Codes/" + "img.bmp"),
System.Drawing.Imaging.ImageFormat.Bmp);

        property.path = Server.MapPath("~/Images/QR_Codes/" + "img.jpg");
        string logoPath = "";

        image = System.Drawing.Image.FromStream(new
MemoryStream(File.ReadAllBytes(property.path)));

        if (fuEmbedLogo.HasFile)
        {
            String fileName = fuEmbedLogo.PostedFile.FileName;
            fuEmbedLogo.SaveAs(Server.MapPath("~/Images/Logos/" + fileName));
            logoPath = Server.MapPath("~/Images/Logos/" + fileName);

            System.Drawing.Image logo = System.Drawing.Image.FromStream(new
MemoryStream(File.ReadAllBytes(logoPath)));

            /* logo resizing begins*/
            int maxLogoWidth = 50, left, top;
            Bitmap resizedLogo = null;

            if (logo.Width > maxLogoWidth)
            {
                int newLogoHeight = (int)(logo.Height * ((float)maxLogoWidth /
(float)logo.Width));
                resizedLogo = new Bitmap(maxLogoWidth, newLogoHeight);
                Graphics gr = Graphics.FromImage(resizedLogo);
                gr.InterpolationMode = InterpolationMode.HighQualityBicubic;
                gr.DrawImage(logo, 0, 0, maxLogoWidth, newLogoHeight);

                left = (image.Width / 2) - (resizedLogo.Width / 2);
                top = (image.Height / 2) - (resizedLogo.Height / 2);

                Graphics g = Graphics.FromImage(image);
                g.DrawImage(resizedLogo, new Point(left, top));
            }
            else
            {
                left = (image.Width / 2) - (logo.Width / 2);
                top = (image.Height / 2) - (logo.Height / 2);

                Graphics g = Graphics.FromImage(image);
                g.DrawImage(logo, new Point(left, top));
```

```
            }
            /* logo resizing ends*/

            image.Save(Server.MapPath("~/Images/QR_Codes/" + "img.jpg"),
System.Drawing.Imaging.ImageFormat.Jpeg);
            image.Save(Server.MapPath("~/Images/QR_Codes/" + "img.png"),
System.Drawing.Imaging.ImageFormat.Png);
            image.Save(Server.MapPath("~/Images/QR_Codes/" + "img.gif"),
System.Drawing.Imaging.ImageFormat.Gif);
            image.Save(Server.MapPath("~/Images/QR_Codes/" + "img.bmp"),
System.Drawing.Imaging.ImageFormat.Bmp);
        }
        else
        {

        }

        using (Bitmap bitMap = new Bitmap(image))
        {
            using (MemoryStream memoryStream = new MemoryStream())
            {
                bitMap.Save(memoryStream, System.Drawing.Imaging.ImageFormat.Png);
                Byte[] bytes = new Byte[memoryStream.Length];
                memoryStream.Position = 0;
                memoryStream.Read(bytes, 0, (int)bytes.Length);
                string base64String = Convert.ToBase64String(bytes, 0, bytes.Length);
                imgQRCode.ImageUrl = "" + base64String;
                Session["isDefaultImage"] = "IsNotDefault"
}
}
```