BIOMETRIC APPLICATION OF INTELLIGENT AGENTS IN FAKE DOCUMENT DETECTION OF JOB APPLICANTS

Salathiel Bogle[1] and Suresh Sankaranarayanan[2]

[1]Mona Institute of Applied Science, University of West Indies, Kingston, Jamaica
salbogleprogmer@gmail.com
[2]Department of Computing, University of West Indies, Kingston, Jamaica
pessuresh@hotmail.com

ABSTRACT

The Job selection process in today's globally competitive economy can be a daunting task for prospective employees no matter their experience level. Although many years of research has been devoted to job search and application resulting in good integration with information technology including the internet and intelligent agent-based architectures, there are still many areas that need to be enhanced. Two such areas include the quality of jobs associated with applicants in the job search by profiling the needs of employers against the needs of prospective employees and the security and verifications schemes integrated to reduce the instances of fraud and identity theft. The integration of mobile, intelligent agent, and cryptography technologies provide benefits such as improved accessibility wirelessly, intelligent dynamic profiling, and increased security. With this in mind we propose the intelligent mobile agents instead of human agents to perform the Job search using fuzzy preferences which is been published elsewhere and application operations incorporating the use of agents with a trust authority to establish employer trust and validate applicant identity and accuracy. Our proposed system incorporates design methodologies to use JADE-LEAP and Android to provide a robust, secure, user friendly solution.

KEY WORDS: *M-commerce, Agents, Cryptography, JADE-LEAP, Android*

1. INTRODUCTION

In today's global economy, the challenges associated with finding a suitable job is amplified by the technicalities associated with the Job search process which is seen by experience. Normally when we want to apply for a job, we search the newspapers; listen to radio and television broadcasts that may advertise vacancies and also job seekers register themselves with job site portals such as Academickeys.com, Monster.com, Careerbuilder.com and so on. Many employers do not register themselves with these mediums to provide full details of the job specifications but instead post important details on their own website only. Also with the growing number of online job search engines, segmenting the online labor market into "information islands", make it almost impossible for job seekers to get an overview of all relevant positions [1]. Thus feasible approaches to improve navigation in job offers and protect the applicant's identity are not only important but they are necessary to help users find job offers more effectively [2]. For many employers, the monetary and non-monetary aspects of jobs are important determinants of the

DOI : 10.5121/ijcseit.2012.2108

number of applicants for jobs. Non-employed job applicants could have more difficulty in getting a job interview than those currently employed but, once interviewed, may not face any further difficulties in getting employment [3]. Therefore job application is a very competitive process in which the applicant's objectives includes successfully obtaining the job for the best negotiated salary and the employer's objectives includes selecting the most capable employee for the lowest negotiated salary [3][4]. Today, the internet plays a major role in job search and application with the launch of Online Career Center around 1993. Since then several mega job search sites have come on stream with Monster.com, a semantic based job search site being one of the most popular with over a million job postings at any time, 63 million job seekers per month in 2008 and over 150 million resumes[5].While it is attractive for site operators to encourage users to post their resume and contact details online, job seekers need to exercise caution as they have no control over where their resume will eventually be seen as their resume could potentially be viewed by fraudsters who may use information from it to a mass and sell personal details or even perpetrate identity theft [5][6]. Security is therefore very important in job application, and knowing the identity of those whom you communicate with in virtual communities is essential for understanding and establishing identity and the effects of identity deceptions and the conditions that give rise to it [6]. It is indeed plausible that job applicants could easily fake identity or achievements, unfairly positioning them in the job market. Also employers could be deceitful in posting fictitious job postings as a scheme to defraud or mislead prospective applicants. With these issues in mind, we will now look into intelligent agent technology and how agents can be used towards job application system which is our proposed work. The paper is organized in sections as follows. Section 2 provides details on Online Job search and Application systems with motivation towards developing an Agent based Job Search system. Section 3 gives details on the Intelligent Agent Technology followed by Agent based utility and Job Search theory. Section 4 talks on Intelligent Agent based Mobile Search system developed followed by Fingerprint matching and Security Schemes. Section 5 talks on Agent based Secure Application System with architecture details and algorithm. Section 6 gives the implementation details on JADE-LEAP and Android 2.2. Section 7 is conclusion and future work.

2. ONLINE JOB SEARCH AND APPLICATION SYSTEMS

Job search and application is not a new area as several significant works have been done in several key areas to modernize, improve security and increase the success and usage of these systems. Some of the works that have inspired the conception of this research include:

- '*Improving Job Search by network of professionals and companies*' research in which job clusters were created to provide relationship between categories of professionals and company needs and is based on a network of job offers, discovering interesting relationships between them and clustering these to represent companies or professional. The output is a visualization of the network of professions and companies [2].
- The '*Semantic Web-based*' recruitment research used the data exchange between employers, applicants and job portals; and is based on a set of vocabularies in ontology which provide shared terms to describe occupations, industrial sectors and job skills. Monster.com uses a similar semantic web-based technology [1].
- '*Agent-based Application for Supporting Job Matchmaking for Teleworkers*' is a multi-agent system that performs job matchmaking in teleworking community focusing on the time consuming task of searching for appropriate working partners [7]
- Risk Aversion and Expected Utility theories which calibrate the relationship between risk attitudes over small and large stakes when the expected utility hypothesis is maintained [8]
- '*Open Source Java Framework for Biometric Web Authentication Based on BIOAPI*' which provides interoperability between different software applications and devices by using the BioAPI specification which allows software applications to communicate with a broad range of biometric technologies [9]

Although these and other research have contributed to the implementation of several web based and android applications including monster.com, seek.com, academickeys.com, careerbuilder.com, LinkUp, HireADroid, etc., there is no work that support an agent based architecture running on JADE and Android that is capable of providing utility based ordering of jobs, dynamic employer rating over period, fuzzy job selection rules [10][11] and secure biometric application with applicant and employer verification which is unique in our system. So taking these into consideration we have developed the Intelligent Agent-based Mobile Job Search and Secure Application system where details on Intelligent agent based Job search system will be discussed in brief and been published elsewhere But before going into system developed we need to review details on Intelligent Agents, Job search Theory, Agent based utility and security considerations towards application system.

3. INTELLIGENT AGENT TECHNOLOGY

Over the years there has been much controversy about the definition of an artificial intelligent agent [12]. There exists a weaker notion of agents and a stronger more controversial notion. [13] define an agent as “anything that can be viewed as perceiving its environment through sensors and acting upon that environment through effectors”. Hayes-Roth (1995) agrees with this definition but adds additional clarity by stating that “intelligent agents continuously perform three functions: perception of dynamic conditions in the environment; action to affect conditions in the environment; and reasoning to interpret perceptions, solve problems, draw inferences and determine actions”. Agents should autonomously carry out activities by being independent or self-directed and should not depend on external input only from human operator or other agents to act manifesting social abilities when interacting with other agents (and possibly humans) via some kind of agent-communication language [12-15]

Today artificial intelligent agents are integrated into many computer-based systems including expert systems, job search engines, web searches, info-bots and so on. These autonomous agents can perform time consuming, mundane and sometimes even life endangering tasks reliably, instead of the human agent [16]. [14] describes a stronger notion of agency in which agents process characteristics such as knowledge, belief, intention and obligation. Other attributes applies to stronger agent notion. These include mobility where agents move around an electronic network, veracity where agents will not knowingly communicate false information and benevolence where the assumption is that an agent will try to do what it is asked and will not have conflicting goals [17]

3.1 Job Search Theory

In a dynamic labor market, the process by which people find new jobs has importance to policymakers and scholars also. Policymakers have made attempts to design training and other programs to help match an individual’s skills with the requirements of potential employers [18]. Job-search theory attempts to propose strategies for making optimal employment decisions by considering factors that determine individual’s demands and their prospect for finding an acceptable job offer [19][20]

Job search models are measured in both discrete and continuous time and a simple model can be used to represent the basic search behavior of an unemployed worker where the intent is to maximize expected utility [20]. This research focuses on Discrete Time Job search. In Discrete Time Job search the individual is interested in choosing a policy (i.e. a sequence of decision rules) that determines whether or not to accept any particular job offer. The eventuality of the job offer is referred to as the outcome and is dependent on preferences of the searcher such as skills, pay, location of the employment opportunity, and the willingness of the employer to employ the searcher. The review of job search theory provides the basis for a discussion on agent-based utility relevant to the job search process.

3.2 Agent-based Utility

In economics, utility functions are used to model preferences of agents. These functions serve as a device for us to assign a single number to any bundle [21]. Proponents of Subjective Expected Utility (SEU) theory have offered many axiomatisations of their models. One approach develops utility and subjective probability as distinct concepts and provide explicit axioms which justify the combination of these into an expected utility ranking of the strategies (options, actions, prospects) before a decision maker [22]. In 1979 weighted utility theory was proposed by Chew and MacCrimmon, and then refined by Chew [23]. Chew replaced the independence axiom with weak independence and convexity axioms which led to a weighted linear representation [23]. Expected utility '**u**' is a linear function on the simplex:

$$\{\mathbf{p} \mid \mathbf{p} = (p_{1,} p_2 ,\ldots, p_n); \sum p_i = 1; \forall\ I, p_i \geq 0\}$$

A prospect (x_1, p_1; …; x_n, p_n) is a contract that yields outcome x_i with probability p_i based on the linear function above. To simplify notation, we omit null outcomes and use (x, p) to denote the prospect (x, p; 0, 1-p) that yields x with probability p and 0 with probability 1-p. The (riskless) prospect that yields x with certainty is denoted by (x). Thus expectation to choose prospects is based on

$$U(x_1, p_1; \ldots ; x_n, p_n) = p_1\, u(x_1) + \ldots + p_n\, u(x_n).$$

That is, the overall utility of a prospect, denoted by U, is the expected utility of its outcomes (Kahneman and Tversky 1979).

4. INTELLIGENT AGENT BASED MOBILE SEARCH SYSTEM

Although online job search sites have greatly improved the job acquisition process there are still challenges in providing a qualitative approach to job search, providing a job best suited for an employee. The main objective of the system developed [10][11] as shown in Fig.1 addresses the following challenges:

- *Intelligent agent (instead of human agent) to perform the job search operations by interacting with employer and job search coordinator agents (Bogle & Suresh, 2011; Bogle & Suresh, 2011).*
- *Agent based utility concept to provide suitability profiling based on configurable factors such as distance from work, days and shift requirements, work environment, safety and hazard considerations, remuneration, skillset, etc.*
- *Employ fuzzy preference rules, to make proper decision in getting a list of jobs corresponding to the user desired specification.*
- *Enable past and current employees to profile employers based on configurable metrics*

There are still some challenges in the system developed towards security concerns in the job application process such as fraud and identity theft of Employee and Employer .So taking these into consideration we here have proposed the application of Biometric – fingerprint matching towards fraud and identity theft which is unique and first of its kind. But before going into the details of system developed, we will review the Fingerprint matching and Security schemes.

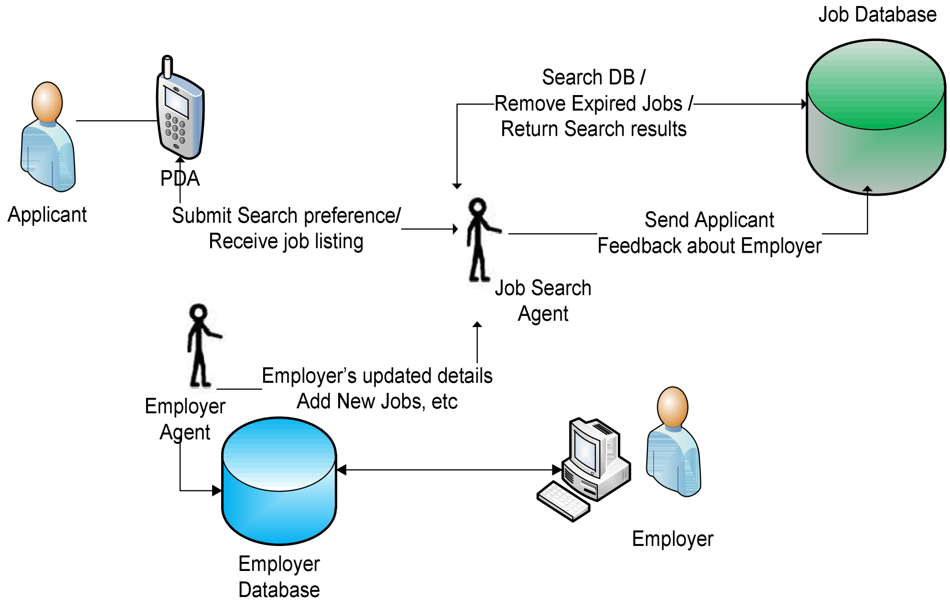


Fig. 1 Job Search Flow Architecture

3.3 Fingerprint Matching

Fingerprints are graphical flow-like ridges present on human fingers [24][25]. The use of fingerprint for identification has been around since 6000 BC. With the increase in small fingerprint devices integrated in mobile devices, laptops, etc. at cheaper costs, it is expected that the use of fingerprint for personal authentication and security will increase [26]. Fingerprint identification is based on two premises: (i) fingerprint details are permanent – based on the anatomy and morphogenesis of friction ridge skin, and (ii) fingerprints of an individual are unique – the notion of fingerprint individuality has been widely accepted based on inspection by experts of millions of fingerprints [27]. [28][29] states that fingerprint matching can be separated formally into the categories of verification and identification. Verification is the comparison of a claimant fingerprint against an enrollee fingerprint, where the intention is that the claimant fingerprint matches the enrollee fingerprint. Identification is the matching of an unknown fingerprint against a database of known and catalogued fingerprints to associate the fingerprint with an identity. This is traditionally used in the domain of forensic criminology [26] In order to perform matching it is critical that an understanding of the structure and features of the fingerprint is obtained.

The lines that flow in various patterns across the fingerprint are called ridges and the spaces between ridges are valleys. The more microscopic of approaches is called minutia matching. The two types are ridge ending and bifurcation. An ending is a feature where a ridge terminates and a bifurcation is a feature where a ridge splits from a single path to two paths at a Y-junction. For minutiae matching purposes a minutia has a location(x, y) and direction (additional features are also possible). Minutia matching, because of deformations in sensed fingerprints, is an elastic matching of point patterns without knowing their correspondences beforehand. Generally, finding the best match between two point patterns is intractable even if minutiae are exactly located and no deformations exist between these two points. The existence of deformations makes the minutia matching much more difficult. Correlation matching can also be used and is also called global matching, simple image multiplication or image subtraction. Simplistically, the process can be thought of as checking if the ridges correspond after aligning two fingerprints and subtracting them [26][27]. Since fingerprints are permanent as discussed above, if they were intercepted during communication or retrieved from an endpoint because of poor security, a perpetrator could effectively fake their identity, pretending based on false biometrics. Therefore good security schemes are extremely important to protect this biometric data.

3.4 Security Schemes and Considerations

Security is the attribute of a system to be safe against attacks or other interference [30][31]. Since a person's fingerprint is very sensitive data, it is very important that this biometric data be protected by using cryptographic techniques [32].There are numerous cryptographic schemes and algorithms available however this research is specifically interested in Certificate based authentication and trust, HTTPS, and AES symmetric key encryption, discussed below.

X.509 certificate is a signed record that associates users' identification with the cryptographic keys and the framework postulates that everyone will obtain certificates from an official certifying authority (CA) usually a Trusted Third Party (TTP). The public-key certificate consists of a data part and a signature part. The data part consists of the name of an entity, the public keys corresponding to that entity, and additional relevant information including the validity period for the public key and so on. The signature part consists of the signature of a TTP over the data part [33].

Hypertext transport protocol secure (HTTPS) is a technology where Secure Socket Layer (SSL) or Transport Layer Security (TLS) is applied as a sub-layer over HTTP. HTTPS automatically encrypts and decrypts data during communication transfer. SSL is designed to make use of TCP to provide a reliable end-to-end secure service [34]. The two most important concepts of SSL are the session and the connection. The specification defines these as follows:

- *Connection:* A connection is a transport that provides a suitable service, For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with a session [33][34]
- *Session:* An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptography security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection [34][35]

The National Institute of Standards and Technology (NIST) worked with the cryptographic community and developed and Advanced Encryption Standard (AES). The overall goal was to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm capable of protecting sensitive (unclassified) government information [36]. The Rijndael proposal for AES was accepted by NIST and defined a cipher in which the block length and the key length can be independently specified to 128, 192 or 256 bits. The AES specification uses the same three key size alternatives but limit the block length to 128 bits. Rijndael was designed to have the following characteristics:

- Resistance against all known attacks including Brute Force attacks
- Speed and code compactness on a wide range of platforms so that the use of the algorithm is practical in a wide range of applications
- Design simplicity [34].

4 INTELLIGENT AGENT BASED BIOMETRIC IN SECURE APPLICATION

The literature reviewed confirms that the technologies exist to create a system that improves the job search process using well founded techniques such as utility theorem applied to autonomous agents, increased accessibility through the use of mobile technology and safeguards against fraud and identity theft by using proven security encryption and biometric techniques such as fingerprint matching, x509 certificates, and AES encryption [36]. This section provides a design for the construction of such a system. The architecture shown in Fig 2, integrates critical components to enable it to work effectively. A data enabled mobile network integrated with a local area network (LAN) is the required platform. This enables efficient agent communication between the mobile device and the multi-agent environment. All agents in the architecture were designed to follow the FIPA2000 architecture for Agent Communication Language (ACL) message passing in multi-agent systems and provide the protocol for managing agent interaction and coordination [37].Let us now discuss the design roles and responsibilities of these components in the architecture.

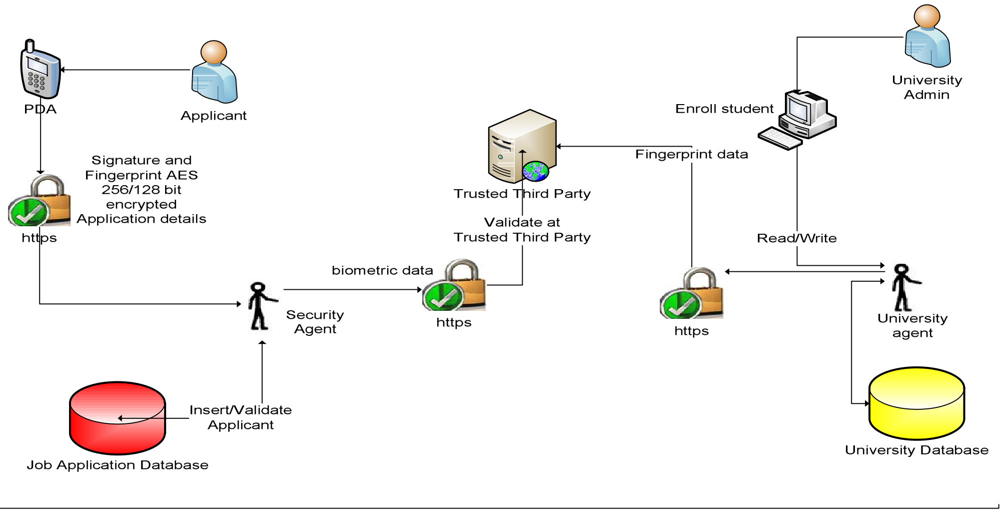


Fig. 2 Job Application Flow Architecture

The Intelligent agent based Secure Application design consists of the five intelligent agents and a trusted third party. Let us now briefly consider these agents:

- **Applicant Agent (AA) -** The applicant agent performs the activities of a human agent for job search and application and is a key entity in the process. The Applicant Agent primary responsibilities are:

  i. Pre-populate relevant job application fields on user screen from registration data.
  ii. Capture and encrypt biometric details for secure transfer over https.
  iii. Securely submit over https, job application details including encrypted fingerprint and signature.
  iv. Liaise with security agent to check if employer is third party trusted and communicate warning to user if employer is not, also giving them the option to abort the job application if the user desires.
  v. Report job application submission status and job application number for future reference.

- **Employer Agent (EA) –**The employer agent models some actions and responsibilities performed by the employer. The main activities are:

i. Interact with the Security Agent and Trusted Third Party in the employer verification phase by providing valid certificates that are third party trusted as input for verification. The employer trusted website certificate if from the known trusted third party, is sufficient to mitigate costs.
ii. Sends job application details excluding biometrics as well as applicant education status results to the human employer.

- **Security Agent (SA) –** This agent is critical in the job application process and provides confidentiality and some nonrepudiation by employing cryptographic functions to securely pass data including biometric fingerprint and applicant signature from the applicant to the trusted third party for verification. The security agent also communicates the job application status to the AA and EA respectively and performs these functions:

i. Establish HTTPS SSL connection with the Applicant Agent for secure transfer of job application data including biometric data.
ii. Establish secure https connection with trusted third party to verify employer certificates using trusted third party APIs.
iii. Establish secure https connection with employer agent to obtain certificate for trust verification.
iv. Receives applicant education status verification results and securely transfers over https connection results to the applicant agent for presentation to the applicant.
v. Securely transfers applicant’s job application details with education status verification but excluding applicant’s biometric data as a report to the employer agent for presentation to the employer.

- **University Agent (UA) –** This agent theoretically interacts on behalf of the university in the verification process between the trusted third party and the university databases. Since each university will have its own legal and security concerns, this abstraction is made to facilitate varying degrees of limitations within the university that impacts the verification process. The core responsibilities are:

i. Interact with the university database in accordance to university policy and procedures relating to student’s confidentiality.
ii. Verify the identity of the trusted third party via its certificate to ensure it is not communicating with a fake or unknown TTP.
iii. Securely liaise with the trusted third party to ensure only authorized applicant education verification requests are processed.
iv. Keep a log audit of all such interactions for the university administration

- **Trusted Third Party (TTP) -** The trusted third party for example VeriSign has the role of securely interacting with the SA, EA and UA agents through certificate based trust schemes and symmetric based encryption to validate biometric data, the existence of education credentials where possible and verify the existence and trust or lack thereof of employers who post jobs to the system. The following role is expected of the TTP:

i. Securely liaise via https with the security agent to securely obtain encrypted biometric and education details for verification and validation.
ii. Securely liaise with the security agent via APIs to validate the employer certificates.
iii. Securely verify applicant identity by biometric data by using fingerprint matching techniques.
iv. Securely liaise with the university agent to verify applicant’s education credentials.

4.1 Job Application Algorithm

The following steps outline the job application process from the system architecture shown in Fig 2 and 3. The flowchart of the process is shown in Fig 4:

- Applicant securely logs-in over https and clicks apply on a job selected from the search process.
- The applicant agent then sends a message to the security agent who checks if the logged in user has already applied for this job. If the applicant had previously applied, their reference number is returned and presented along with a message that they have previously applied and their application was submitted to the employer. The process then stops.
- If the applicant had not previously applied for the job, the security agent liaises with the employer agent and trusted third party APIs to verify if the employer is trusted. If employer is untrusted, the applicant is alerted by the applicant agent and allowed to decide on stopping or proceeding with the application process.
- The applicant agent auto-complete on the job application screens, some relevant data such as applicant's name, address, telephone, email, etc. from the registration process. This information is editable and can be modified by applicant at any time.
- Applicant agent collects all inputs including captured biometric fingerprint and signature data for submission over https.
- Biometric fingerprint and signature data are encrypted using public key AES 256bit or 128bit encryption depending on the capabilities of the mobile device prior to submission over https.
- Applicant agent submits all inputs via https to the security agent.
- The security agent updates the databases with the application details.
- The security agent liaises with the trusted third party to verify applicant's education details.
- The trusted third party confirms if the employer is a trusted employer. If the employer is untrusted, the trusted third party reports to the security agent that it is unable to perform the requested checks for security reasons as the employer is not third party trusted and stops the verification process.
- If the employer is trusted, the trusted third party then securely liaise with the university agent over https to obtain university copy of applicant's fingerprint and or signature data and relevant summary education details in the format of full-name, year and award obtained for each award obtained.
- The university agent can choose to respond with details or deny request based on strict university policy, or if university is primarily paper base or do not have biometric data of students.
- If the request is denied, the trusted third party will report to security agent that it is unable to verify the applicant education details but with a reason of university does not permit.
- If the request is serviced, the trusted third party then decrypt and verify the applicant biometric data to confirm if the reported awards from applicant are consistent with the university records.
- If they do not match the trusted third party reports to security agent that it is not able to verify the applicant biometric details or the education details. If they do match and are verifiable, the trusted third party reports to the security agent that it is able to verify the applicant's biometric and education details.
- The security agent then communicates verification status very succinctly to the applicant agent allowing for zero proof of knowledge as to reason for verification incase the applicant may be fake or fraudulent.

- The security agent also communicates securely to the employer agent applicant details and verification status and *non-inflammatory or prejudicial reason* for current status to trusted employers only. No biometric data is transferred to the employer agent.
- The applicant agent then facilitates the presentation of this asynchronous communication to the applicant comprising of applicant number and verification status without reason.
- The employer agent also sends an asynchronous communication to the employer of the job application submitted by the applicant including job application reference number and also verification status with reason to the trusted employer only.

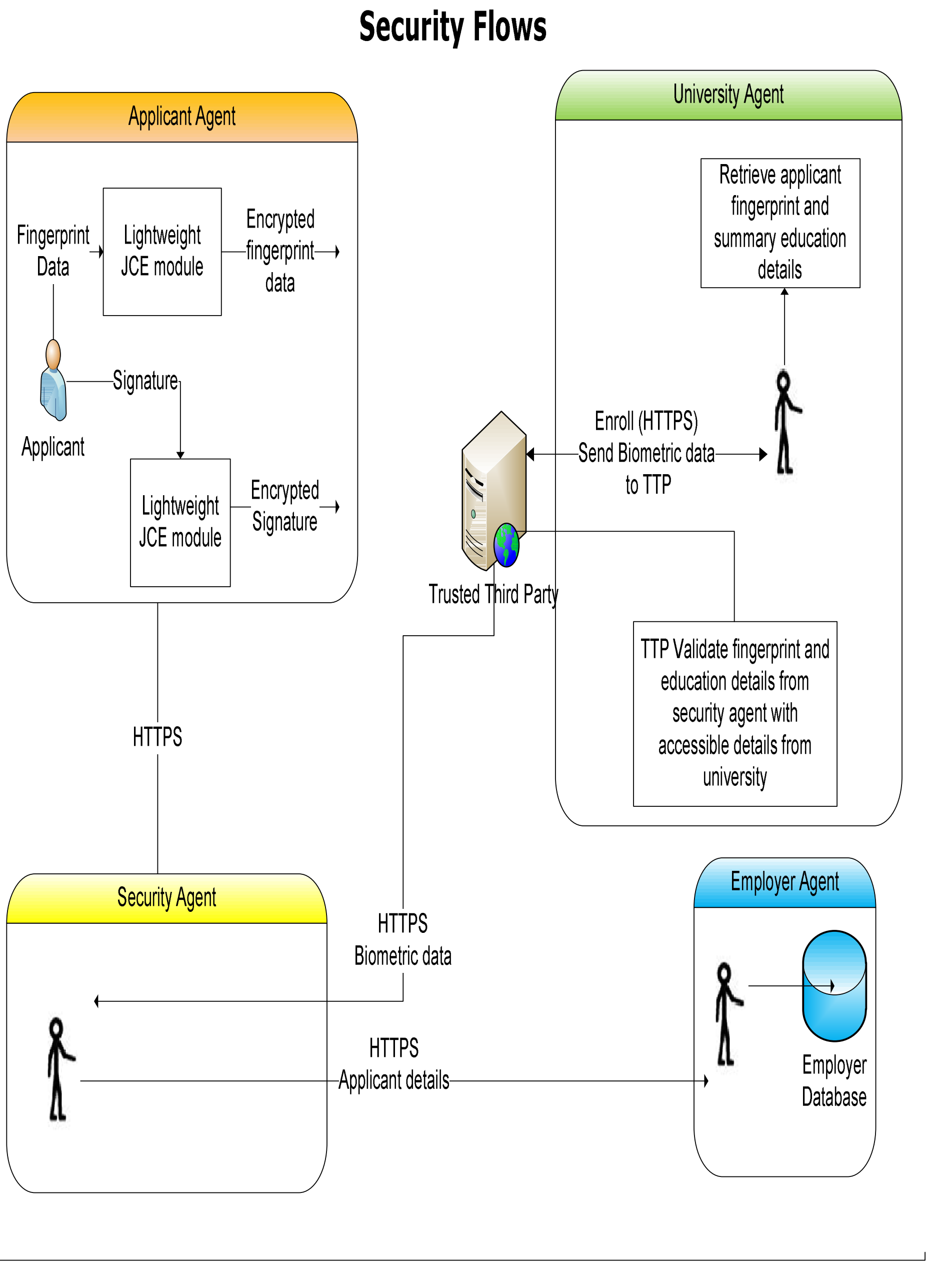


Fig. 3 Security Flow Architecture

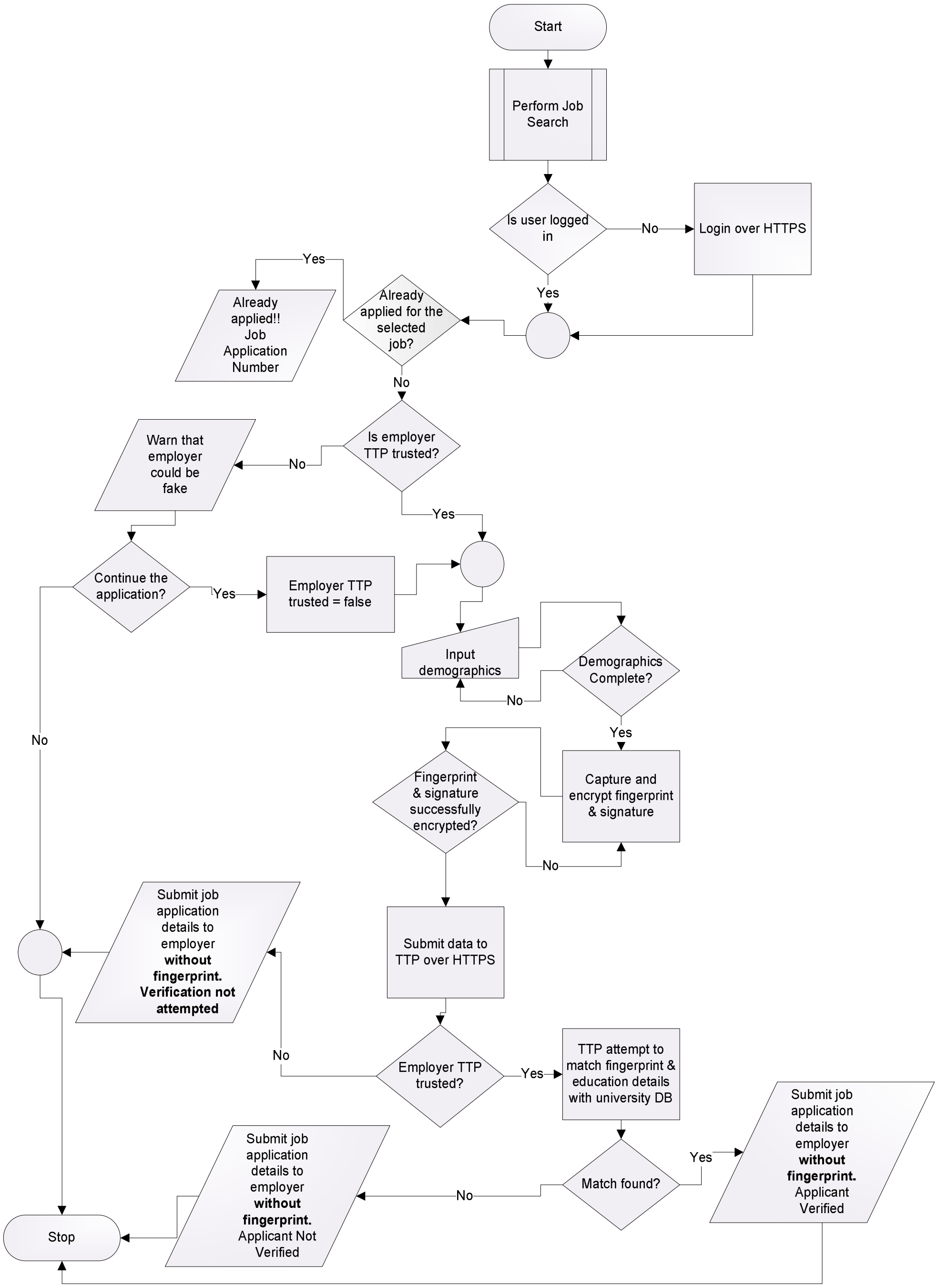

Start
Perform Job Search
Is user logged in
No
Login over HTTPS
Yes
Already applied for the selected job?
Yes
Already applied!! Job Application Number
No
Is employer TTP trusted?
No
Warn that employer could be fake
Yes
Continue the application?
Yes
Employer TTP trusted = false
Input demographics
Demographics Complete?
No
Yes
Capture and encrypt fingerprint & signature
Fingerprint & signature successfully encrypted?
No
No
Submit data to TTP over HTTPS
Submit job application details to employer without fingerprint. Verification not attempted
Employer TTP trusted?
No
Yes
TTP attempt to match fingerprint & education details with university DB
Match found?
Yes
No
Submit job application details to employer without fingerprint. Applicant Verified
Submit job application details to employer without fingerprint. Applicant Not Verified
Stop

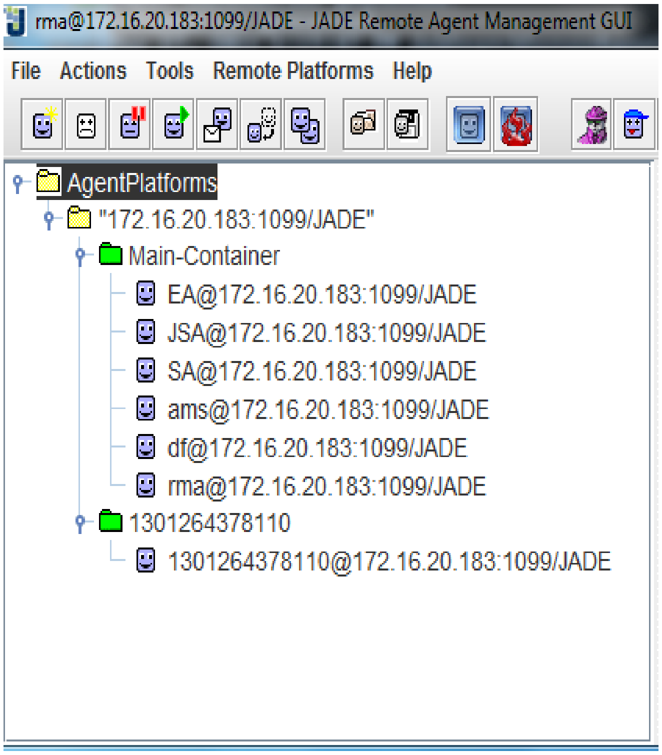
Fig. 4 Job Application Flow

The details on the implementation of the agents based on the architecture presented using JADE-LEAP in Android 2.2 has been presented in Section 4 as screenshots.

5 IMPLEMENTATION USING JADE-LEAP

The system was implemented using java development kit 1.6.0_21 (jdk1.6.0_21) as the base runtime environment using Eclipse Helios release build 20100617-1415 with android plug-in enabled as the development IDE. JADE 4.0.1 was used for the Agent Platform [38] to host all agents, control behavior and perform agent management. JADE-LEAP 4.0 was used to enable agents on mobile devices [39], and Jade Android 1.0 enabled JADE-LEAP agents on Android mobile devices [31]. Android 2.1 platform 8 with Google APIs SDK was used for the creation of the Android application with Google Maps integration capabilities .The Bouncy Castle jdk16-145 lightweight JCE extensions for lightweight cryptography functions including symmetric encryption, public key encryption, and certificate based authentication on Android mobile devices, along with jdk1.6.0_21 Key tool were leveraged for the creation and signing of public key certificates and for establishing the backbone of the system's cryptographic security. GRFingerJava 4.5 fingerprint matching API provided a means to simulate the fingerprint matching facilities based on design architecture in Section 3 that could be used by the trusted third party. Finally MySQL5.1 Database Server using MySQL Workbench 5.2CE was used to create all databases for employer, university, job search & application and trusted third party.

The list of agents in the JADE environment is shown in Fig.5. The Applicant agent resides in a separate split container and labeled with the mobile handset's IMEI number. All other agents reside in the main container and are identified by their abbreviated names.

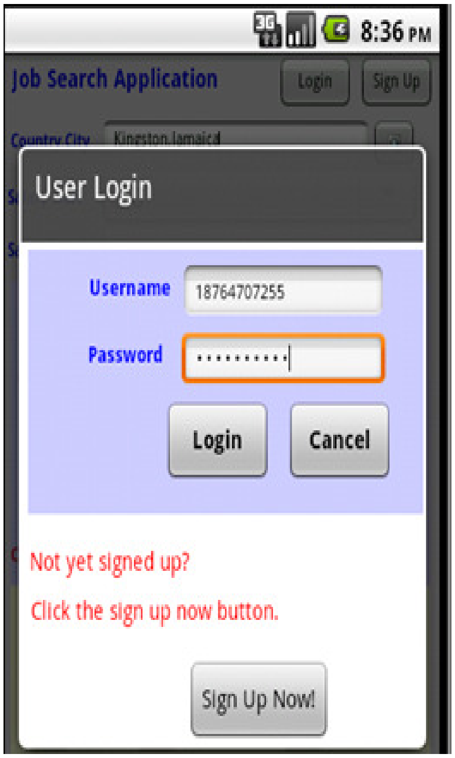

rma@172.16.20.183:1099/JADE - JADE Remote Agent Management GUI
File
Actions
Tools
Remote Platforms
Help

AgentPlatforms
"172.16.20.183:1099/JADE"
Main-Container
EA@172.16.20.183:1099/JADE
JSA@172.16.20.183:1099/JADE
SA@172.16.20.183:1099/JADE
ams@172.16.20.183:1099/JADE
df@172.16.20.183:1099/JADE
rma@172.16.20.183:1099/JADE
1301264378110
1301264378110@172.16.20.183:1099/JADE

Fig.5. Agents in JADE Container

5.1 Job Application Implementation

In order to apply for a job , an applicant must be securely signed in to the system over HTTPS with a valid username and password as shown in Fig. 6.



User Login

Username 18764707255

Password ••••••••••

Not yet signed up?

Click the sign up now button.

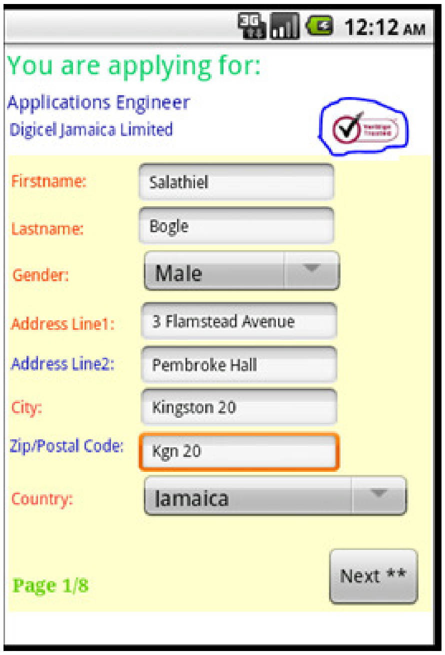
Fig. 6 User Log-in Screen

The applicant demographic and biometric screens are configured as mandatory. Screens that capture supplementary data useful for the applicant digital resume profile like his personal details, Education, Work Experience etc are optional and can be updated at any time. Let us now consider the activities involved in the secure job application process. In this section also there are several scenarios possible from the design but let us discuss the following four (4) scenarios and their screenshots.

1. Employer is third party trusted
2. Employer is not third party trusted
3. Applicant details were successfully verified
4. Applicant details could not be successfully verified.

5.1.1 Employer is third party trusted

An employer is considered third party trusted if and only if their company's existence is validated based on trusted certificates obtained from the trusted third party. For this system the trusted third party is VeriSign. Fig. 7 shows the trust icon obtained by a verified employer after the Security agent securely connects to the VeriSign over HTTPS and uses APIs to validate if the Employer certificate obtained from the employer agent is still valid and was authentic and issued by same trusted third party. Only trusted employers will trigger an applicant details validation by VeriSign with the University.



You are applying for:

Applications Engineer
Digicel Jamaica Limited

Firstname: Salathiel
Lastname: Bogle
Gender: Male
Address Line1: 3 Flamstead Avenue
Address Line2: Pembroke Hall
City: Kingston 20
Zip/Postal Code: Kgn 20
Country: lamaica

Page 1/8

Fig. 7 VeriSign trusted Employer

5.1.2 Employer is not third party trusted

If an employer does not have a valid certificate, for example their website certificate; or the employer uses another trusted third party not supported by the system, the employer will not be validated as third party trusted as shown in Fig.7. Applicants can still choose to submit their applications securely to untrusted employers if they have some reason to trust these employers; however a strong caution is given before allowing submission. This ensures legally that the decision to give untrusted employer who could really be fake, access to their personal demographic details only such as name, telephone, email, belongs only to the applicant. Biometric data is never given directly to an employer and applicants cannot adjust this security level via a configuration. On receiving the alert that the employer is untrusted, the applicant can cancel the application process to protect their demographic data from unknown and fake employers.

5.1.3 Building the Digital Resume

The system demonstrates data capture mechanism for customer demographics and additional details, where portions of this data such as name, email address, telephone number, and so on is auto-completed by the system from data captured in the registration process. All applicants must provide the data to ensure that the employer has the most recent data on the applicant. The system allows for the creation of an electronic resume. The sections currently captured by the system include education details, work experience, hobbies, and references..

5.1.4 Acquiring and encrypting biometrics

No biometric data is stored on the applicant’s mobile to reduce the incident of biometric fraud in the event the mobile device is stolen or used by multiple persons to access the system. A mobile device with a front facing camera or fingerprint scanner is recommended. The system facilitates the capture of a signature using the device touch screen and a stylus. The signature is then encrypted using AES 128/256 bit encryption scheme as shown in Figs. 8 to 11. Since the sensitivity of fingerprint data is not time bound, it is important that the fingerprint is captured, scan quality verified, encrypted, and transferred over HTTPS with any cache removed from the handset. Fig. 37 and 38 demonstrates the screens for capturing fingerprint from the device camera and encrypting using AES 256bit encryption - recommended. A weaker AES 128 bit can be used if the device cannot support the 256 bit encryption. All encryptions for signature and fingerprint are automatically done when transitioning to the next screen if not yet encrypted by clicking on the encrypt button.

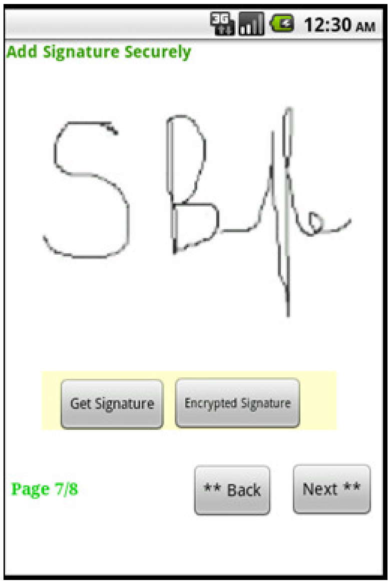


Fig. 8 Applicant's Signature

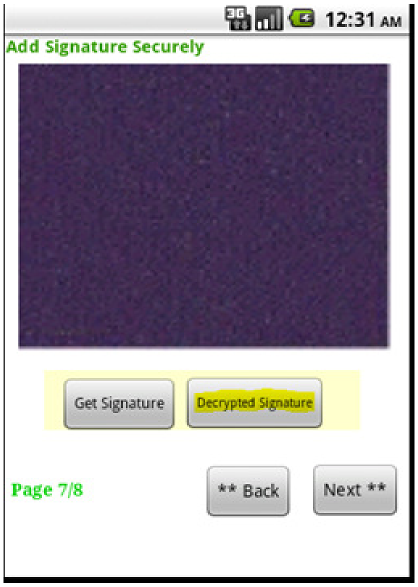


Fig. 9 Encrypted signature

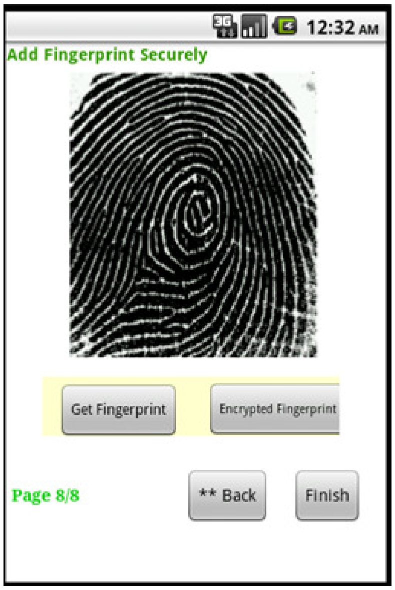


Fig. 10 Applicant's Fingerprint

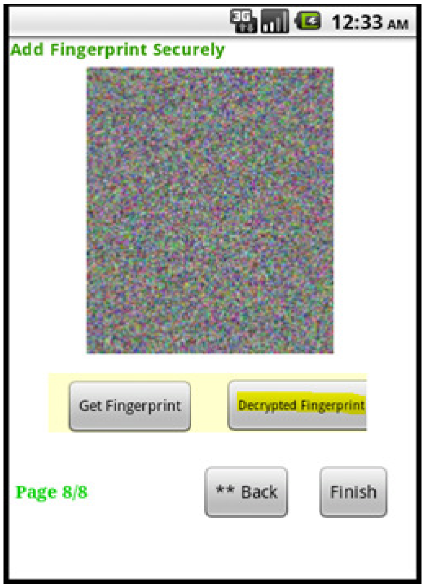
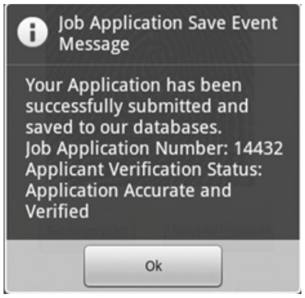


Fig. 11 Encrypted fingerprint

6.1.5 Applicant details successfully verified

In this scenario, the employer is trusted, and the applicant made good effort to provide accurate education, work experience and reference details. The security agent then securely connects over

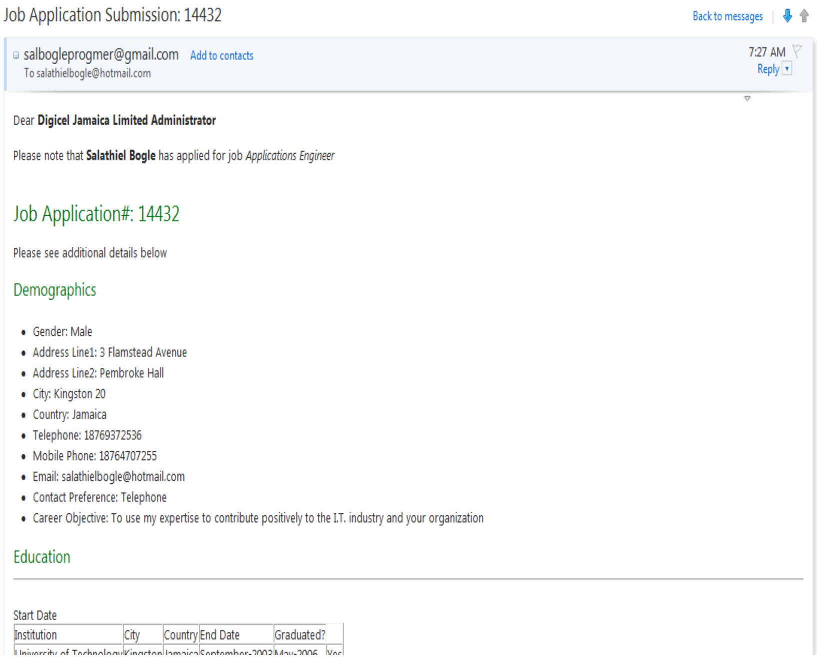
HTTPS to the trusted third party VeriSign and provides biometric details along with relevant demographics and education details to perform the applicant verification with the University agent. VeriSign requests encrypted fingerprint and confirmation of education obtained for the applicant from the University agent. The fingerprint is successfully matched and the degree obtained was confirmed. Fig. 12 shows the message returned to the applicant including job application number for reference and confirmation of details. Fig. 13 illustrates sample communication sent to the Employer for the job application.



Job Application Save Event Message

Your Application has been successfully submitted and saved to our databases.
Job Application Number: 14432
Applicant Verification Status: Application Accurate and Verified

Fig. 12 Job Application Message to Applicant



Job Application Submission: 14432

salbogleprogmer@gmail.com

To salathielbogle@hotmail.com

7:27 AM

Dear **Digicel Jamaica Limited Administrator**

Please note that **Salathiel Bogle** has applied for job *Applications Engineer*

Job Application#: 14432

Please see additional details below

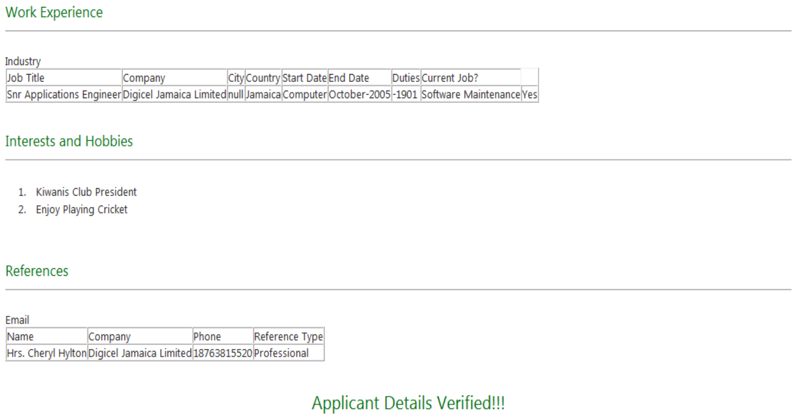
Demographics

- Gender: Male
- Address Line1: 3 Flamstead Avenue
- Address Line2: Pembroke Hall
- City: Kingston 20
- Country: Jamaica
- Telephone: 18769372536
- Mobile Phone: 18764707255
- Email: salathielbogle@hotmail.com
- Contact Preference: Telephone
- Career Objective: To use my expertise to contribute positively to the I.T. industry and your organization

Education

Start Date

Institution	City	Country	End Date	Graduated?	
University of Technology	Kingston	Jamaica	September-2003	May-2006	Yes



Work Experience

Industry

Job Title	Company	City	Country	Start Date	End Date	Duties	Current Job?	
Snr Applications Engineer	Digicel Jamaica Limited	null	Jamaica	Computer	October-2005	-1901	Software Maintenance	Yes

Interests and Hobbies

1. Kiwanis Club President
2. Enjoy Playing Cricket

References

Email

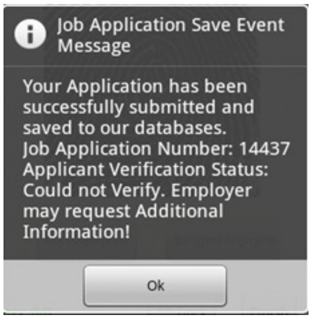
Name	Company	Phone	Reference Type
Hrs. Cheryl Hylton	Digicel Jamaica Limited	18763815520	Professional

Applicant Details Verified!!!

Fig. 13 Job Application Sent to Employer

6.1.6 Applicant details could not be verified.

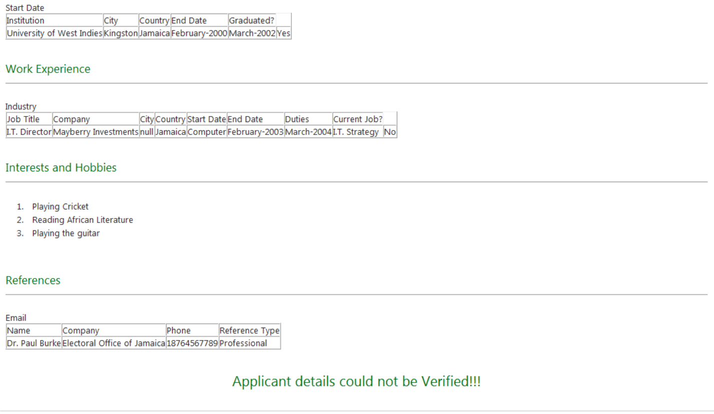
If the employer is not third party trusted, or the applicant fakes information, or the university does not have proper databases with fingerprint, or do not allow trusted third party interaction with university databases as a rule, the applicant details will not be verified. It is the responsibility of the trusted third party to react gracefully and communicate these details to the security agent for an appropriate action to be taken. In this instance, the applicant adds false education to their electronic resume and the security agent engage the trusted third party to attempt verification of the applicant and education details but the university agent was unable to find education details or master degree award listed in resume and returns encrypted fingerprint and empty education details. VeriSign verifies the fingerprint as the applicant's fingerprint but cannot match the education details and reports this to the security agent. Fig. 14 show the message displayed to the applicant along with the job application number and Fig. 15 illustrates the communication sent to the employer.



Job Application Save Event Message

Your Application has been successfully submitted and saved to our databases.
Job Application Number: 14437
Applicant Verification Status: Could not Verify. Employer may request Additional Information!

Fig. 14 Message sent to the applicant



Start Date

Institution	City	Country	End Date	Graduated?	
University of West Indies	Kingston	Jamaica	February-2000	March-2002	Yes

Work Experience

Industry

Job Title	Company	City	Country	Start Date	End Date	Duties	Current Job?	
I.T. Director	Mayberry Investments	null	Jamaica	Computer	February-2003	March-2004	I.T. Strategy	No

Interests and Hobbies

1. Playing Cricket
2. Reading African Literature
3. Playing the guitar

References

Email

Name	Company	Phone	Reference Type
Dr. Paul Burke	Electoral Office of Jamaica	18764567789	Professional

Applicant details could not be Verified!!!

Fig. 15 Employer receive application - Failed verification status

6 CONCLUSION & FUTURE WORK

To demonstrate the soundness of our proposed system, we developed a fully functional prototype using JADE-LEAP running on Android, integrating Google Maps API, and lightweight JCE security APIs to create our Applicant, Job Search, Security, Employer, and University Agents that would securely communicate in a multi-agent environment and with an external third trusted party via HTTPS and APIs to provide intelligence and services demonstrated in the screenshots above. The system also determined if employers are trusted or not and how to verify applicants and react using varied degrees of verification (fully verified, employer not trusted, university does not have biometrics, records partially match, not verified and so on).The perceived drawbacks of the system are the cost that could be associated with the use of trusted third party APIs for employer certificate checks and also fingerprint verification. The reliance on the university to provide applicant matching fingerprint data and education details, as some universities may not willingly distribute student records, or even want to keep biometric details on students. The Intelligent Agent-based Secure Application system can be improved by enhancement of Employer interaction through mobile interfaces developed in Android. Extend android application towards intelligent agent-based virtual secure job interview. This could form the initial basis of a pre-interview before a face-to-face interview if needed to facilitate quick and affordable interviews for applicants from different geographic locations for example and so on. Last but not the least the statistical analysis of fake applicants can be recorded for mitigating such problems in the society.

References

[1] Mochol, M et al(2007). "Improving the accuracy of job search with semantic techniques." Berlin, Germany.

[2] Frivolt, G, and Maria B.(2006) Improving Job Search by Network of Professions and Companies. Bratislava, Slovakia: Institute of Informatics and Software Engineering

[3] Manning, A. (1999) Pretty Vacant:Recruitment in Low-Wage Labour Markets. London: London School of Economics and Political Science

[4] Mason, G (2000). "THE MIX OF GRADUATE AND INTERMEDIATELEVEL SKILLS IN BRITAIN: WHAT SHOULD THE BALANCE BE?" Discussion Paper No. 16, page 11

[5] Wikipedia. 2011. http://en.wikipedia.org/wiki/Employment_website (accessed April 15, 2011).

[6] Donath, J S (1997). Identity and deception in the virtual community. California: Berkeley: University of California Press

[7] Sugawara, K (2003) "Agent-Based Application for Supporting Job Matchmaking for Teleworkers." Second IEEE International Conference on Cognitive Informatics (ICCI'03), pp. 137

[8] Rabin, M (1999). Risk Aversion and Expected-Utility Theory: A calibration Theory. Berkeley California: Department of Economics

[9] Agulla, E at al(2007. An Open Source Java Framework for Biometric Web Authentication Based on BioAPI. Vigo, Spain: Department of Signal Theory and Communications, University of Vigo

[10] Bogle, S and Suresh, S(2011a) . "Intelligent Agent based Job Search and Secured Application System in Android Environment." , Proceedings of 2011 IEEE International conference on Electro/Information Technology. Mankatto, Minesotta, USA.

[11] Bogle, S and Suresh, S(2011b) "Job Search system in Android Environment- Application of Intelligent Agents", Communciated to International Journal of Ubiquitous Computing and Intelligence.

[12] Franklin, S, and Graesser, A(1996). " Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents." Third International Workshop on Agent Theories Architectures and Languages. Springer-Verlag.

[13] Russell, S J., and Norvig, P(1995). Artificial Intelligence: A Modern Approach. Englewood Cliffs, NJ: Prentice Hall

[14] Jennings, N. R., and Wooldridge, M (1998). Applications of Intelligent Agents. London: University of London.

[15] Hayes-Roth, B (1995). "An Architecture for Adaptive Intelligent Systems." Artificial Intelligence: Special Issue on Agents and Interactivity, 329-365

[16] Poole et al (1998). Computational Intelligence. New York: Oxford University

[17] Spanoudakis,N and Pavlos M (2007). "An Ambient Intelligence Application Integrating Agent and Service-Oriented Technologies." In Proceedings of SGAI Conference. Paris, France. pp.393-398

[18] Addison,J et al (2004) . Key Elasticities in Job Search Theory: International Evidence. IZA

[19] Job Search Theory (2004). http://www.ssc.upenn.edu/~rwright/courses/oss.pdf (accessed 04 02, 2011).

[20] Zaretsky, A. M. and Coughlin, C. C. (1993). An introduction to the Theory and Estimation of a Job-Search Model.Review, 53-56.

[21] "Handout on Utility Function Transformation (2002)." Utility Transformation: Intuition.. http://www.econ.umn.edu/~golya002/downloads/3102/Sp09/3102_Handout_Utility.pdf (accessed 04 02, 2011).

[22] Rabin, M. (1999). Risk Aversion and Expected-Utility Theory: A calibration Theory. Berkeley California:Department of Economics

[23] Chew, S. H (1980). Two representation theorems and their application to decision theory. Vancouver: University of British Columbia.

[24] Pfitzmann, B, and Ahmad-reza, S (1996). Anonymous fingerprinting. Berlin: Springer-Verlag.

[25] Jain, A et al(1997). "On-Line Fingerprint Verification." IEEE Transactions on Pattern Analysis and Machine Intelligence VOL. 19, No. 4, pp.302-305

[26] O'Gorman, L (1999). Fingerprint Verification. New Jersey: Verdicom Inc.

[27] Pankanti, S et al(2001). "On the Individuality of Fingerprints." IEEE Transactions on Pattern Analysis and Machine Intelligence ,1010-1025.

[28] Ratha et al.(1996) "A Real-time Matching System for Large Fingerprint Databases." Michigan.

[29] Xiao, Q., and Raafat, H(1991). "Fingerprint image postprocessing: A combined statistical and structural approach." Pattern Recognition, 24(10), 985-992

[30]Cardelli, L. (1999). Mobility and security. Microsoft Research.

[31] Speckmann, B (2008). The Android mobile platform. Michigan: Eastern Michigan University, 2008.

[32] Gordon, M and Suresh, S(2010). "Biometric Security Mechanism in Mobile Payment Systems. Proceedins of 2010 IEEE International Conference on Wireless and Optical communication Networks. Colombo, Srilanka

[33] Menezes, A et al (1996). Handbook of Applied Cryptography. CRC Press

[34] William, S (2005). Cryptography and Network Security Principles and Practices, Fourth Edition. Prentice Hall

[35] Blaze, M et al(1996). Decentralized Trust Management. AT&T Research

[36] Nechvatal et al (2000). Report on the Development of the Advanced Encryption Standard (AES). National Institute of Standards and Technology

[37] FIPA ACL Message Structure Specification (2002)." Foundation for Intelligent Physical Agents. 12 03, 2002. http://www.fipa.org (accessed 2011).

[38] Bellifemine, F et al (2007). Developing multi-agent systems with Jade. John Wiley & Sons, Ltd

[39] Moreno et al (2003). "Using JADE-LEAP to implement agents in mobile devices." http://jade.tilab.com/papers/Exp/02Moreno.pdf. (accessed 2011).

Authors

Salathiel Bogle receive his Master's degree in Computer Science from University of West Indies, Jamaica in 2011. Prior to that he did Bachelor's Degree in Computer Science from University of Technology Jamaica. He is presently working in reputed Telecommunication industry in Jamaica i.e. Digicel as Project Manager. He has got a Research publication in IEEE proceedings from his Master's Dissertation. His research interests are mainly on intelligent agents, Mobile computing.

Dr. Suresh Sankaranarayanan holds a PhD degree (2006) in Electrical Engineering with specialization in Networking from the University of South Australia. Later he has worked as a Postdoctoral Research Fellow and then as a Lecturer in the University of Technology, Sydney and at the University of Sydney, respectively during 2006-08. He is the recipient of University of South Australia President Scholarship, towards pursuing the PhD degree programme and has also bagged the IEEE travel award in 2005. He was working as a Lecturer (Asst. Prof. status) in the Department of Computing and lead the Intelligent Networking Research Group, in the University of West Indies, Kingston, Jamaica, during 2008-11.
He has also worked as a Professor, School of Computer Science and Engineering, Vellore Institute of Technology (VIT University), Chennai Campus, India, for a short period during 2011. He is now working as Associate Professor, Department of Computer & Information Systems, Institute of Technology, Brunei (ITB – A technological university). Currently he is also functioning as a Visiting Professor, Department of computing, Faculty of Pure & applied Science**,** University of West Indies, Mona Campus**,** Kingston-7, Jamaica, West Indies. He has supervised 28 research students leading to M.Sc, ME, M.Phil and M.S degrees. He has got to his credit, as on date, about 50 fully refereed research papers published in the Proceedings of major IEEE international conferences, as Book Chapters and in International Journals. He is also a Reviewer and Technical Committee member for a number of IEEE Conferences and Journals. He has conducted many tutorials, workshops and also given Guest Lectures in Networking in various Universities and Colleges. He also managed a collaborative research programme with Oakland University, Rochester, USA. His current research interests are mainly towards 'Mobile and Ubiquitous Computing - Wireless Sensor Networks, Mobile Commerce, Intelligent Agents' used in the Health, Commercial and Engineering sectors.