NoSQL: Confidential on Data Security and Data Management by Using a Mobile Application

Hemn B. Abdalla, Jinzhao Lin, Guoquang Li, and S. Mushhad M Gilani

***Abstract*—CV data is one of the most precise forms of information for job seekers (or) employees details about personal, professional and both It manages and maintains any organization securely. Ensuring the security of data is, therefore, critical not only to preserve the data's of employees' highly personal information but also to minimize the legal risk to the organization as a whole. When some organizations do not see the full details of the job seekers CV, so for that we have to provide the security for this CV. When an organization takes care of reducing the manual workload, an organization performs; they choose to replace those processes with various levels of security systems. Data Security is the keeping data protected from corruption and unauthorized access and focuses beyond data security is to ensure the privacy while protecting personal or (business) corporate data. This paper will manage the complexity of CV data's. It's had a various process like employees develop their personal and organizational skills, knowledge, and abilities. Security is of high aspect when it comes to choosing a human resources management system, especially when it means keeping company (corporate) data and the privacy of employee records safe from hackers. Using a method of secure transmission of Encrypting and Decrypting Messages which encrypts the data as it transmits over the job portals with exchanging securely cryptographic keys over a public channel. An important is security is hiding of users particular details. Using NoSQL(MongoDB) for Saving and retrieve our data details.**

***Index Terms*—NoSQL, data security, encryption, hiding of data's, key generation.**

I. Introduction

The history of recruitments (or) job seeking dates back to World War II. Early recruitment methods involved a direct interview, Intelligence Quiz Test, and Personal Interviews, in which its need did not arise of targeting candidates as there was a surplus supply of labor. Later the methods like advertisement, publishing & headhunting were used to target relevant candidates. It was not before 19th Century that job-portals came into existence aiming to provide a "one-stop-shop" for job seekers & employers. Many Job seeking portals are there; use of these portals is searching or recruiting the matching profile to the particular job [1]. Nowadays the company or any organization wants the employees means they are not conducting the direct walk-ins. Just there are given the ad for job portals. Already In these job portal lakes of resumes to uploaded. The job portal recruiters are seeing that profile and recruit the matching profile. In this stage, all the recruiters see our CV data's. So avoiding that particular field only they want to view. So we have to provide the security for this our proposed system. A job search engine is a website that facilitates job hunting. In job portal itself several categories are theirs. Simply recognized as job boards and range from big scale generalist boards to excellent job boards for groups such as engineering, legal, insurance, social work, teaching and seasonal Jobs, users can typically deposit their resumes and submit them to potential employers. Cryptography used in an information technology security can keep our personal details and environment to protect data that is sensitive. Secure data anywhere it goes, especially on mobile (wireless) devices from laptops and USB drives to smartphones and tablets. Trend Micro's integrated data protection (prevention) solutions make it easier to identify, track, and secure sensitive about the company, customer details, and employee data from the endpoint to the cloud. The Data Security Manager changes the data security management game by functioning the IT organization to have a consistent and repeatable method for encrypting, enforcing access policies, and gaining or obtaining the security intelligence for all structured and unstructured data. The Data Security Manager is in place, new security policies, compliance requirements, and risks are quickly met through the Vormetric Transparent Encryption, Vormetric Application Encryption, or managing keys and certificates that can provide for 3rd party devices. The final result of centralizing is a control of such a breadth of data-at-rest security standards costs low of the ownership, enough deployment of new secure services, and an increase in control and visibility of data across your organization. We are applying a Diffie-Hellman algorithm for providing the security for encryption your CV data details. ElGamal Algorithms for Encrypting and Decrypting Messages between users consists the key generator. Standard security solution to data is done by encrypting the data [2]. NoSQL(MongoDB) for applying large-scale data that saves all personal CV job seeker details on our server, MongoDB are quickly grown to become a popular database for web applications and Mobile application, more importantly NoSQL is fast data access [3], [4].

Manuscript received August 30, 2015; revised November 25, 2015.

The authors are with Chongqing University of Posts and Telecommunication, China (e-mail: hemn.db85@yahoo.com, linjz@cqupt.edu.cn, ligq@cqupt.edu.cn, mushhad@uaar.edu.pk).

II. Research Aim

How do we keep our CV documents secure? To achieve this objective we introduce a layer structure as illustrated in Fig. 1. In this section we elaborate the functionality through a series of checks and balances:

A. Limited Access

When documents are placed on our servers, data access is limited only fixed IPs to come into the system by a firewall.

B. Track Users

The custom designed system allows us to track all system users and ensures that only those people with security policies are accessing the system.

C. Document Tracking

We provide version control and document access history. Any time change is made to the text; the new version is saved and backed up immediately.

D. Off-site Redundancy

We backup for all data off-site at a secure location. File redundancy ensures that, should our experience server problems of any kind, your data is safely backed up off-site.

1) Keyword search and Boolean search
2) Experience Search
3) Location criteria
4) Education Criteria
5) Freshness of the resume (Showing resume in chronological order as updated by the candidate).

Let the Careers Portal help you find a job within your chosen field of study. We have the latest graduate programs with companies like Telkom, Transnet, Eskom, Sasol, Nedbank and many more. Graduate applications offer an excellent opportunity for work based experience after you've completed your studies and can set you on the path to your chosen.

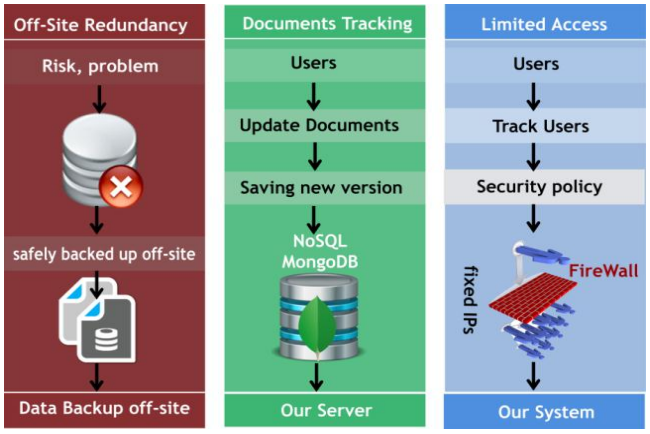


Fig. 1. A layered approach to keep CV documents secure.

III. Methodology

A. Diffie-Hellman Algorithm

In this CV's data, we are providing the security for encryption. Encryption means the one form of data (readable data) to another form of data (unreadable data). To over the encryption is applying the Diffie-Hellman algorithm. Use of this algorithm is the encryption scheme depends upon the private and public key pairs.

Encryption of data requires the private cryptographic key. Encryption is the standard means of rendering a communication private [5], [6]. The most challenging part in this type of Encryption is the transformation of the encryption key from the sender to receiver without anyone intercepting this key in between. The key varies the user independently.

This transfer or generation of same cryptographic keys at both sides secretively was made possible by the Diffie-Hellman algorithm, as shown in Fig. 2.

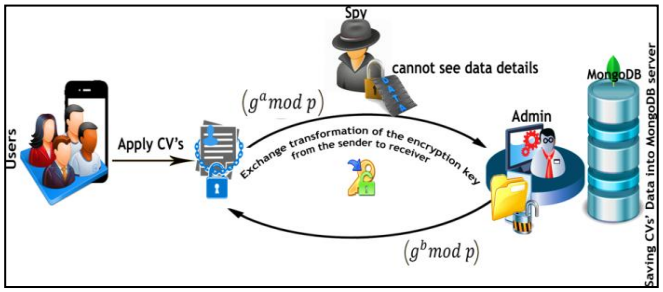


Fig. 2. Diffie-Hellman exchanging key between users.

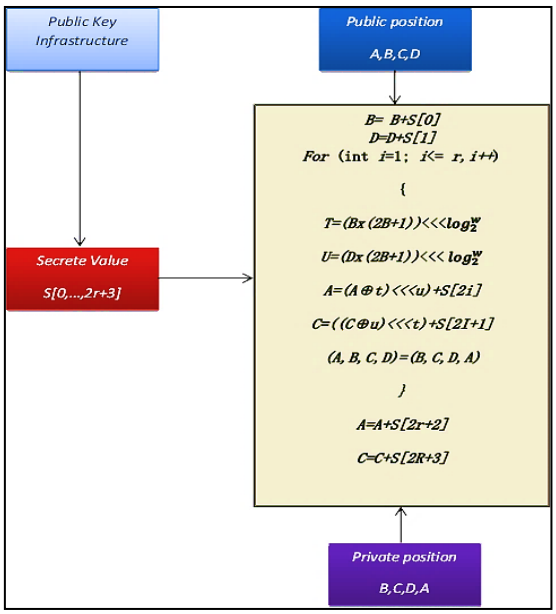


Fig. 3. Implement code diagram.

Fig. 3 shows the Encryption data (Transformation key from the sender to a receiver).

B. ElGamal Algorithms

The ElGamal cryptographic algorithm is one of the few probabilistic encryption schemes. However, its security has never been concretely proven based on clearly understood and accepted primitives [7], [8]. It is mainly used to establish standard keys and not to encrypt messages.

- *Encrypting and Decrypting Messages:*

If "HEMN" now wants to send a message to "HASTI", he randomly picks a number k that is smaller than p, then computes:

$$e_1 = g^k \bmod p \tag{1}$$

$$e_2 = A^{k*}\, m \bmod p \tag{2}$$

and sends e_1 and e_2 to "HASTI". "HASTI" can us this to reconstruct the message m by computing

$$e_1^{-a} \times e_2 \bmod p = m \tag{3}$$

Because

$$\begin{aligned} e_1^{-a} \times e_2 \bmod p &= (g^k)^{-a} \times A^k \times m \\ &= g^{-a*k} \times A^k \times m \\ &= (g^a)^{-k} \times A^k \times m \\ &= A^{-k} \times A^k \times m = 1 \times m = m \end{aligned}$$

- *Code Implementation for Elgamal Encryption:*

```
package key_distribution_center;
import java.math.*;
public class Diffie_Hellman
        {
//Elgamal Encryption
public static String   key_exchange(String c11,String xx,
String pp)
{
BigInteger c1 = new BigInteger(c11);
BigInteger p = new BigInteger(pp);
BigInteger x = new BigInteger(xx);
BigInteger k2 = c1.modPow(x, p);
System.out.println("Signature");
System.out.println("K2= "+k2);
return k2.toString();
 }
 }
```

IV. Output and Experimental Setup

We implemented the Confidential on Data Security and Data Management without SQL and Query as a Mobile application system using Java language with JSP. The Mobile application interface for our system forms used open-source JavaScript library, we used MongoDB for saved our data's information details. All experiments were run using Android system for the mobile application and machine with Intel Core 3CPU @2.9GHz, 4096G main memory, and running on Windows 10 Pro.

Shown one of CV Data in our server:


```
{
   "_id" : ObjectId("55e972687fb8d55477d9f802"),
   "HRname" : "deepa",
   "HRemail" : "*****@gmail.com",
   "HRmob" : "18302337271",
   "HRcname" : "CQUPT",
   "HRclocation" : "chongqing",
   "Username" : "he",
   "Uemail" : "***@yaoo.com",
   "Umob" : "123456789",
   "Ulocation" : "cqupt",
   "Ukeyskill" : "Mongodb",
   "Uexperience" : "2",
   "Urelawantdomain" : "MONGODB",
   "role" : "Java",
   "anualsalary" : "3000",
   "status" : "waiting"
}
```


Shown one of ResumeData (JAVA.CHUNK) in our server:


```
{
   "_id" : "55e970ca7fb8d55477d9f7fd",
   "filename" : "cv1.docx",
   "aliases" : null,
   "chunkSize" : NumberLong(262144),
   "uploadDate" : ISODate("2015-09-04T10:22:02.928Z"),
   "length" : NumberLong(476208),
   "title" : "software developer",
   "contentType" : "application/msword",
   "md5" : "2919f58c53cb7ef4d165240cdddc1f0f"
}
```


TABLE I: Data Description

No.	CVs Document Name	CVs File Size in MongoDB	CVs File Size in Our local Driver	Secret Key
1	CV1	0.23KB	469KB	5440
2	CV2	0.25KB	471KB	710915
3	CV3	0.22KB	468KB	91602
4	CV4	0.25KB	468KB	1476
5	CV5	0.45KB	491KB	4903
6	CV6	0.45KB	491KB	8965
7	CV7	0.44KB	490KB	2197
8	CV8	0.23KB	469KB	63251
9	CV9	0.19KB	465KB	39015
10	CV10	0.25KB	471KB	92013
11	CV11	0.27KB	473KB	24577
12	CV12	0.29KB	475KB	59749
13	CV13	0.32KB	477KB	92592
14	CV14	0.21KB	467KB	67884
15	CV15	0.22KB	468KB	19333

In Table I shown data details on our server with an apply secret key by Elgamal algorithm and get secret key from the cloud to who's apply CV's documents and different data size between original size with original documents size in our server MongoDB.

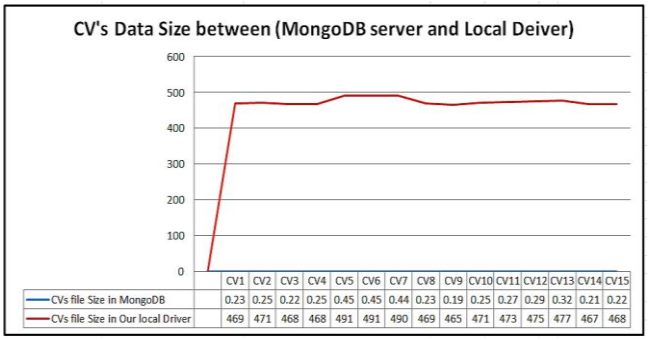


Fig. 4. CV's data size between (MongoDB & Local Driver).

In Fig. 4 chart showing, the files storage and size for each one of them in the particular local driver and MongoDB server. With the different CV files the size of them.

In Fig. 5 representation in our system application how users execution and run our method.

In Fig. 6 shown how our system is running, first users try to use user ID with password after first step user can upload his\her CV details, Second steps our data features automatically save in MongoDB server with running the ElGamal cryptographic algorithm for Encrypting and Decrypting Messages and provide with getting the Secret key from cloud, third steps the private and public key pairs by apply Diffie-Hellman algorithm for transformation key from the sender to receiver with hiding some important details part

of CV's data, fourth steps Mapping process for value mappings between two return data models. Whenever the users want to retrieve or find the his\her document after inputting his phone number, they can directly get his\her own CV files or by an administrator user.

Fig. 5. Screenshot confidential on data security and data management.

V. Conclusion

To develop the security for the personal CV data's, it is certainly possible to take care of the functions are manual, an automated system ensures there is plenty of time available for the human resources are staff to develop and maintain the data that goes into those systems. Each company is different from other systems available on the market to choose from the wider areas of job searching facilitate the quick and easy way access to opportunities. The increasing job opportunities and changing scenario of the business environment today have made more peoples to search for better professional jobs and career and employers to search for better potential. So, in this situation we have to provide the security for this data. Moreover, providing the security for CV data control is on another clue. This situation has prompted many employees to move to job portals to look for the ways that have been widely accepted and fully useful in job searching purpose. In this sense, the job portals assume greater importance, and we could develop such an efficient system that used for many job hunters and employers. This system has been prepared successfully which incorporate all the requirements. This site designed in such a way that any further modifications needed can be easily done. The job seekers like this type of technique because their personal data will be recovered from some third party hackers. Getting a huge different to reduce data size between original document sizes with saving documents size in our server MongoDB.

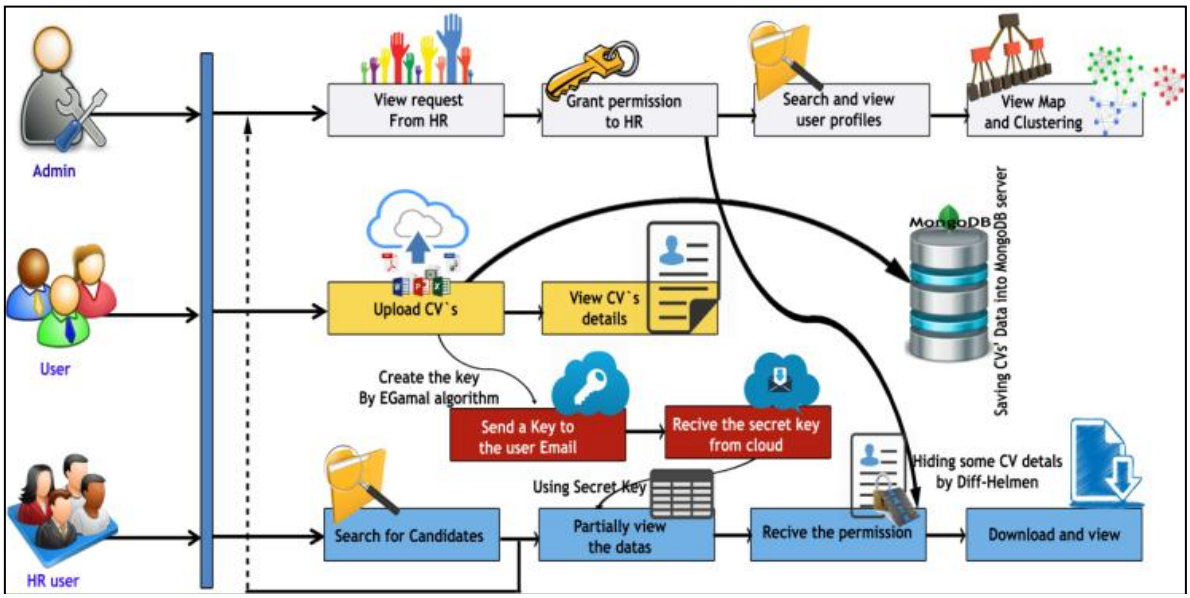


Fig. 6. Implementation diagram our system.

Acknowledgment

This research work is supported by University Innovation Team Construction Plan of Chongqing, the National Science Foundation of China under Grant No. 61301124.

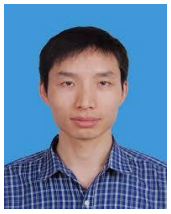
References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, pp. 120-126, 1978.
[2] A. Zahid, R. Masood, and A. S. Muhammad, "Security of shared NoSQL databases: A comparative analysis," in *Proc. Information Assurance and Cyber Security*, 2014, pp. 1-8.
[3] M. Paryasto, A. Alamsyah, and B. Rahardjo, "Big-data security management issues," in *Proc. Information and Communication Technology*, 2014, pp. 59-63.
[4] G. Iachello, "Protecting personal data: Can IT security management standards help?" in *Proc. the 19th Annual Computer Security Applications Conference*, 2003, pp. 266-275.
[5] Y. Tsiounis and M. Yung, "On the security of ElGamal based encryption," *Lecture Notes in Computer Science*, vol. 1431, pp. 117-134, 1998.
[6] P. Rewagad and Y. Pawar, "Use of digital signature with diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing," in *Proc. Communication Systems and Network Technologies)*, 2013, pp. 437-439.
[7] A. Armoni, "Data security management in distributed computer systems," *Informing Science, Data Security*, vol. 5, no. 1, pp. 19-27, 2002.

[8] R. Singh and S. Kumar, "Elgamal's algorithm in cryptography," *International Journal of Scientific & Engineering Research*, vol. 3, issue 12, pp. 1-4, 2012.

Hemn Barzan Abdalla received the master degree in computer science from Huazhong University of Science and Technology, in 2014. Currently, he is a Ph.D. student at Chongqing University of Posts and Telecommunication (CQUPT). His research interests include big data and data security, NoSQL, application.

Jinzhao Lin received his Ph.D. degree in 2001 from Chongqing University. Since 2003, he has been a professor at Chongqing University of Posts and Telecommunications (CQUPT). His current interests include wireless communications and ASIC design.



Guoquan Li received his Ph.D. degree in the College of Communication Engineering from Chongqing University (CQU), Chongqing, China in 2012. He is currently a lecturer with Chongqing University of Posts and Telecommunications, Chongqing (CQUPT), China. His research interests include digital baseband signal processing, multi-user MIMO system, coding theory and technology.

Sed Mushhad Mustuzhar Gilani is currently a Ph.D. scholar in the School of Computer Science at Chongqing University of Posts and Telecommunication, China. He obtained MS (computer science) degree from IQRA University Islamabad, Pakistan. In April 2005, he joined University Institute of Information Technology, PMAS-AAUR where he is serving as an assistant professor. His research interests include software-defined networking, future Internet architecture and mobile networks.