American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-9, Issue-5, pp-71-81
www.ajer.org
Research Paper Open Access

An Improved Cloud-Firewall Model for Detecting and Preventing Data Leakage on Email Platforms

Onuodu, Friday Eleonu[1]andNwoka, Abigail Eberechi[2]
[1]*Department of Computer Science, University of Port Harcourt, Nigeria, gonuodu@gmail.com*
[2]*Department of Computer Science, Ignatius Ajuru University of Education, Nigeria, nwokaabigail@gmail.com*
Corresponding Author: Onuodu, Friday Eleonu

ABSTRACT : *There is an alarming rate of data leakage on Email Platforms. This is because; not every Email Platforms user takes security seriously. There are basically two major data leakage problems which include Malicious Data Leakage (MDL) and Inadvertent Data Leakage (IDL) respectively. Despite various improvements on data security by different encryption algorithms, there are still open problems and occurrences of data leakages on Email platforms. In this work, we developed an Improved Cloud-Firewall Model for detecting and preventing data leakage on Email Platforms. We adopted Structured System Analysis and Design Methodology in this approach. Our proposed model shows that fraudulent data leakage can be blocked through Internet Protocol (IP) scanning and message notification to the Email User. The results obtained showed efficiency in Time Complexity especially in areas which include speed in access validation of Email Platforms users and the speed in data leakage detection. The values for the evaluated parameters are 19 and 12 seconds respectively as compared with the Existing System values of 37 and 45 seconds, which clearly indicates that the proposed system outperforms the Existing System in quick response time. The work could be beneficial to Email users and Software Developers that require relevant information on the prevention of data leakages to hackers.*

KEYWORDS:*Data Leakage, Cloud-Firewall, Model, URLs, Internet Protocol, Email Platforms*

Date of Submission: 08-05-2020 Date of acceptance: 22-05-2020

I. INTRODUCTION

Not every Email Platforms user takes security seriously. Email Platforms Usage (SMU) in the world today has grown exponentially. Indeed, we can boldly attest that the world is becoming a unique global village. However, SMU has attracted corrosive effects to users as a result of data leakage. Data leakage can be defined as a data breech that results to an unintentional release of secure information to an un-trusted environment. Secondly, most Email Platforms users click on pop-up adverts, and are mandated to fill out forms in order to access certain site locations. Hence, confidential data is leaked to an un-trusted third-party without proper investigation. There is an urgent need for an improved model toprevent data leakage on Email Platforms. Data leakage on Email Platforms causes problem to numerous users as there is an increase in the occurrence of the incident. Hence, the application of improved model of data leakage detection system will execute the role of monitoring different interactive platform on the web, and further collect information about Unified Resource Locators (URLs) according to the user's preference.

Digressing a little, there have been reported cases of workers leaking classified data through Email Platforms. Improper use of Email Platforms causes detrimental impacts on users in terms of vulnerabilities to cyber-criminals for data leakage. Interestingly, most profiles on Email Platforms are surprisingly made available to be downloaded from torrent sites, exposing more than 170 million users' information globally [1]. According to Archana et al [2], "Cyber-criminals are now interested in formation gathering of big data. Some of them are sponsored by certain parties to do extremely complex cyber-attacks in order to steal sensitive and classified data. In addition, they use available information in public domain, especially online Email Platforms to gather as many information on special individuals before launching spear-phishing and special engineering techniques to obtain credentials for accessing the valuable information". Confidential user information can be found in a document collection section. Thus, in order to protect these documents, the need for data encryption is highly indispensable. The concept of data leakages and detection should be a collective effort for all stakeholders of the

data management sector, and also Email Platforms users on Facebook, Instagram and Twitter. Also, the encryption of the data is aided by the cryptographic module that resides on the clients' server, while all the other services reside in a cloud. The search module is applied to discover web pages that might indicate data leakage. The application of a search module for potential data leakage threat is essential for Email Platforms users. This is because the purpose of the search module is for locating web pages that shows any sign of potential data leakage. Secondly, the search module is implemented as a conventional keyword-based meta-search engine. Another function of search module includes the dropping of search queries to several other search engines are further combined into a single list, thereby improving the effectiveness and scope of the results. Another cardinal point of this study is the need for situation awareness on data leakages on Email Platforms. Situation awareness can be described as the perception of the element of an environment in terms of time and space, the understanding of their meaning, and the projection of their status in future. Several researchers on the issue of Situation Awareness have perceived the role of poor planning and decision making [3]

We also defined information leakage as "a breach of the confidentiality of information, typically originating from staff inside an organization and usually resulting in internal information being disclosed into the public domain" Although information leakage or unauthorized information disclosure can be caused by malicious and non-malicious insiders, non-malicious insiders are the greater problem since accidental security incidents happen more often and have greater potential for harm than malicious insider attacks. While information can be leaked through offline social networking such as meetings, conferences and publications, the leakage through Online Social Network (OSN) is fundamentally different than its offline counterpart. This is because the moment employees post sensitive information on their sites, the published information is almost permanent, it can be reached by many people and, possibly be copied and distributed to someone else. If they leak information face-to-face to someone, possibly due to the slip of a tongue, the information is confined to the people who heard the conversation, and even if it is communicated to other people, it becomes hearsay.

1.2 Overview of Data Leakage

Data leakage can be described as the process of leaking sensitive and confidential information intentionally or unintentionally to unauthorized parties. It can be private or public information. The root cause of data leakage can be caused by malicious and non-malicious insider attacks. This is because; a non-malicious insider could hardly be expected based on their everyday action. In other words, they are not suspected to be harmful or a source of threat to an organization. The importance of data leakage can be verified in the area of data security, especially if it is caused by an insider, which has seriously threatened security and personal privacy. However, there are some traditional technologies for preventing data leakages. These technologies are mainly based on domain that is segmented into security sub-domains according to data protection requirements, and limitthe data flow between security domains through Cloud-Firewall, encryption and terminal control.

There are some vectors that are responsible for high-level data leakages. This is because; the relinquishing of data to un-trusted parties can be attributed to several ways. It is very necessary that transmission through all other possible channels being recognized in order to prevent data leakage. Most data leakage breaches emanate from internal sources from hackers. Several platforms for data leakage can be identified as instant messaging, email, web mail, Gmail, yahoo, hot mail, web logs, malicious web pages, hiding in SSL, removable media devices, security classification errors, hard copy, cameras, inadequate file protection, and inadequate database security. Furthermore, the need for adequate classification of data security is highly indispensable. These security classifications reflect the urgency in handling of the classified information whether it is restricted, confidential, and secret or top secret in any cases. After all, there is also need for national data security. These measures should be taken seriously by Email Platforms users, security agencies, and software developers, and data analysts. Another reason for this is that poor data security portrays a bad picture in data handling.

1.3 Cloud-Cloud-Firewall Model

In computing, a cloud-cloud-Cloud-Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A cloud-Cloud-Firewall typically establishes a barrier between a trusted internal network and un-trusted external network, such as the Internet.

Cloud-Cloud-Firewalls are often categorized as either network cloud-Cloud-Firewalls or host-based cloud Cloud-Firewalls. Network cloud-Cloud-Firewalls filter traffic between two or more networks and run on network hardware. Host-based cloud-Cloud-Firewalls run on host computers and control network traffic in and out of those machines. The term cloud-Cloud-Firewall originally referred to a wall intended to confine a fire within a building. Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment.

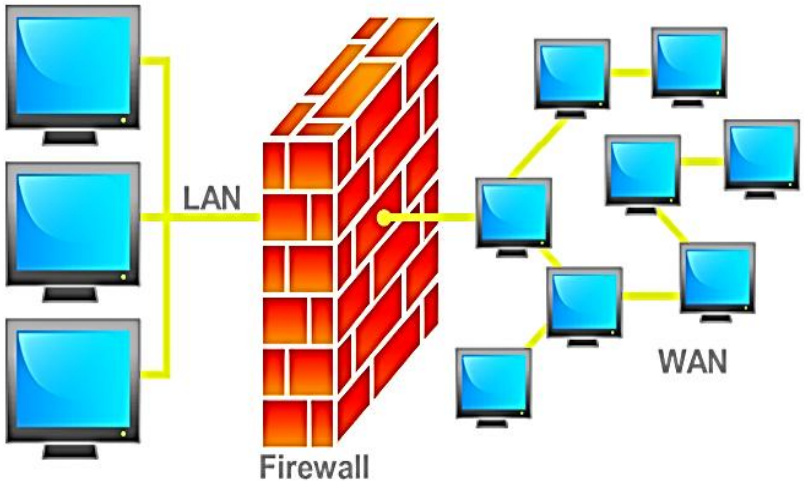

Fig. 1.1: An illustration of where a Cloud-Firewall would be located in a network (Source: [3])

The term was applied in the late 1980s to network technology that emerged when the Internet was fairly new in terms of its global use and connectivity. The predecessors to cloud-Cloud-Firewalls for network security were the routers used in the late 1980s, because they separated networks from one another, thus halting the spread of problems from one network to another.

II. RELATED WORKS

Chandni et al [1] researched on data leakage detection. The work analyzed how a distributor of datasets dispatches confidential data to agents in order to reduce the leakage of data. In other words, a data distributor releases confidential data to trusted agents. The work adopted soft computing methodology, but was limited in stating the main framework for data leakage and prevention.

Archana et al [2] looked at data leakage detection. The study proposed useful strategies in terms of data allocation which improves data leakage detection or identification. The study also illustrated that lots of responsibilities fall in the hands of the distributor. Also, data leakage is handled by water marking technique which requires modification of data. The work adopted Structured System Analysis and Design Methodology. However, it did not state an improvement measure for data leakage prevention.

Adrienn [3] researched on DATALEAK: Data Leakage Detection System. The author further emphasized on a semantic information retrieval-based approach to data leakage on websites. The aim of his model was to monitor the web and collect information about web documents according to users' preferences. The collected Web data sources are compared with user's confidential documents. If a document turns up on the Web that is semantically similar to confidential user documents the system indicates potential data leakage. However, major drawbacks identified from the work include absence of a prevention technique for malicious data leakage, absence of data visualization technique for any potential threat of malicious data leakage, and also the absence of a cloud server in the model.

Mica [4] looked at a theory of situation awareness in dynamic systems. The work presented a model for situation awareness in terms of data leakage detection. It further suggested that there is need of exploring the relationship between situation awareness and individual factors. The work adopted Software Development Lifecycle Methodology. However, we were not able to cite the comparison performance of his result to other systems performances.

Prerna [5] looked at the implementation of data leakage detection using agent guilt model. The study recommended that every agent with datasets to share should be adequately profiled in order to prevent the issue of data leakage. The work adopted Structured System Analysis and Design Methodology. However, the work failed to enumerate real-life implementation examples for the model technique mentioned.

Chirag [6] developed the Detection and Prevention of Data Leakages on web servers. The work discussed data leakages in most web servers as an uncontrolled or unauthorized transmission of classified information to the outside. However, data leakage detection systems cannot provide absolute protection. Thus, it is essential to discover data leakage as soon as possible. In addition, the work adopted Structured System

Analysis and Design Methodology. However, there was no adequate comparative analysis of results to show the benefit of his proposed study.

Atif [7] researched on Information Leakage through Email Platforms; opening the doorway for Advanced Persistence and Threats. He illustrated that Data leakage is the big challenge in front of the industries and different institutes. The work adopted Soft Computing Methodology. However, there was no comparative analysis of results.

Krubhala [8] researched on online social network: a threat to privacy and security of human society. The work provided an overview to users' privacy management from threats such as users' block, design pitfall and limitations, implicit flows of information, and clash of stimulus. The work adopted Agile Methodology but its results were complex to understand.

Mohamed [9] researched on social networks: Privacy Issues and Precautions. The work investigated and discussed issues in terms of privacy and security in data protection on social networks. The study also proposed some useful measures that should be applied to tackle the issues. The work adopted Agile Methodology. There was no program implementation and output in order to shed more light to the discussed study

Reddy et al [10] looked at Data Leakage Detection using Cloud Computing. The work presented the conception of data leakage, its causes of leakage and different techniques to protect and detect the data leakage. The value of data is incredible, so it should not be leaked or mishandled. Furthermore, the work adopted Rapid Application Development Methodology (RAD). However, the benefits of the work were not deployed to Email platform Platforms.

III. MATERIALS AND METHODS

3.1 Methodology

Structured System Analysis and Design Methodology (SSADM) was adopted in this approach

3.2 Analysis of the Existing System

The Existing System we intend to analyze is DATALEAK: Data Leakage Detection System as carried out by [3] and further illustrated in figure 3.1. The goal of the DATALEAK system is to monitor the Web and collect information about Web documents according to users' preferences. The collected Web data sources are compared with user's confidential documents. If a document turns up on the Web that is semantically similar to confidential user documents the system indicates potential data leakage. Usually, the similarity of documents is determined using a repetition-based hard similarity metric. The Existing System approach ignores all potential semantic correlations between different words. In our system not the pure content, but the meaning of Web documents and user documents are compared. The system consists of a number of modules. The document collection contains sensitive, protected or confidential information. In order to protect these documents, encryption is required.

The Cryptographic module is responsible for preparing an encrypted version of the documents. Regarding the confidential content of the documents, the Cryptographic module resides on the clients' server. All the other services reside in a cloud. The Search module is responsible for discovering Web pages that might indicate data leakage. The Search module incorporates a Crawler module that investigates the structure of Web sites, determines those pages of Web sites that contain relevant data, and indexes these pages using keywords. The Text mining module converts Web documents into their appropriate mathematical representation. The Scoring module matches the mathematical representations of Web documents and confidential user documents. In addition to the Existing System analysis, methods that are used in the Text mining, Cryptographic and Scoring module are presented. Web documents and confidential user documents, the scoring module computes a relevance score that measure the similarity between these documents. The scoring module uses different mathematical representations of documents. The Existing System has the following:

- **Web Data Sources:**

This component represents sources of datasets that are developed with the help of semantic web tools, and allows information sharing through HTTP protocol.

- **Confidential Data:**

This component represents discrete data that an individual protects from unauthorized bodies.

- **Data Leakage Detection Model:**

This component represents a system that detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring and detecting. Furthermore, the data leakage detection model consist of two sub components namely the "data leakage" and "no problem". When there is similarity between confidential data and generally used data, then data leakage has occurred, otherwise no problem.

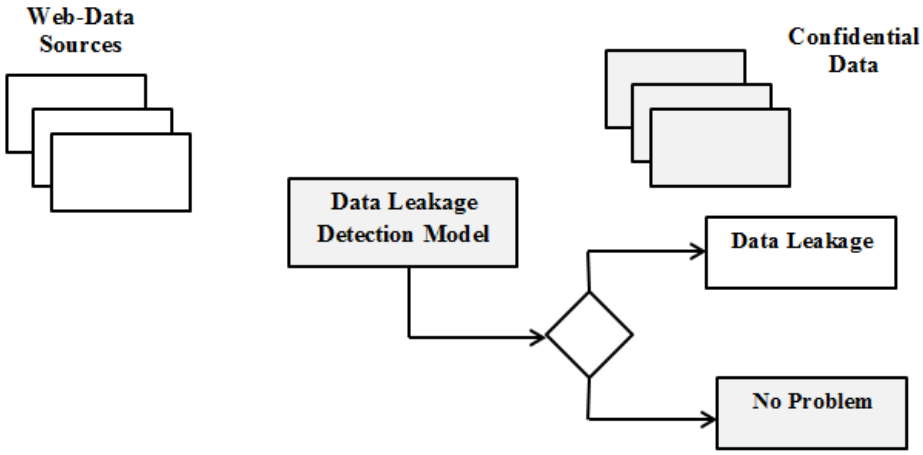

Fig. 3.1: Existing System Architecture of DATALEAK: Data Leakage Detection System (Source: [3])

3.2.1 Disadvantages of the Existing System

The following disadvantages of the Existing System are:

i) Unavailability of Malicious Data Leakage Prevention Technique:

The lack of prevention techniques such as improved cloud-Cloud-Firewall models and water-marking in the Existing System can trigger unauthorized transfer of classified information from a computer or datacenter to the outside world which can also be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding (steganography).

ii) Lack of a Data Visualization Technique for Evaluating the System Performance:

Lack of this technique will cause the existing system not to be able to evaluate data in form of images and animations. Furthermore, the mentioned drawback can cause exploitation of vulnerability in a publicly exposed service, through tricking a user into opening an infectious attachment, or even causing automated

3.3 Analysis of the Proposed System

We intend to improve the existing system with an Improved Cloud-Cloud-Firewall Model which scans, block and visualize potential data leakage threats on email platform figure 3.2. We intend to achieve the proposed system through simulation using web-based programming tool, a relational database management system and Dynamic Programming Algorithm (DPA). This improvement will enable email platform users to screen any advert that requires the input of confidential and classified information. Also, the newly improvement of the existing system will also support its deployment to mobile web application usage on Smartphones. Another uniqueness of the Proposed System includes the awareness on Email platform Security. Furthermore, the proposed system design involves a combination of logical/technical-, physical- and personnel-focused countermeasures, safeguards and security controls. The proposed system also advocates that cyber-security should be defined in a security policy, verified through evaluation techniques (such as vulnerability assessment and penetration testing) and revised, updated and improved over time as the organization evolves and as new threats are discovered.

The proposed system has the following:

i) An Improved Cloud-Cloud-Firewall Detection Model:

This component enhances the process of malicious data leakage detection and prevention through an automated IP address scanner and blocker for malicious and fraudulent links on email platform. It is an online model that receives internet service from the cloud server, and further visualizes potential data threats which comes in form of image links.

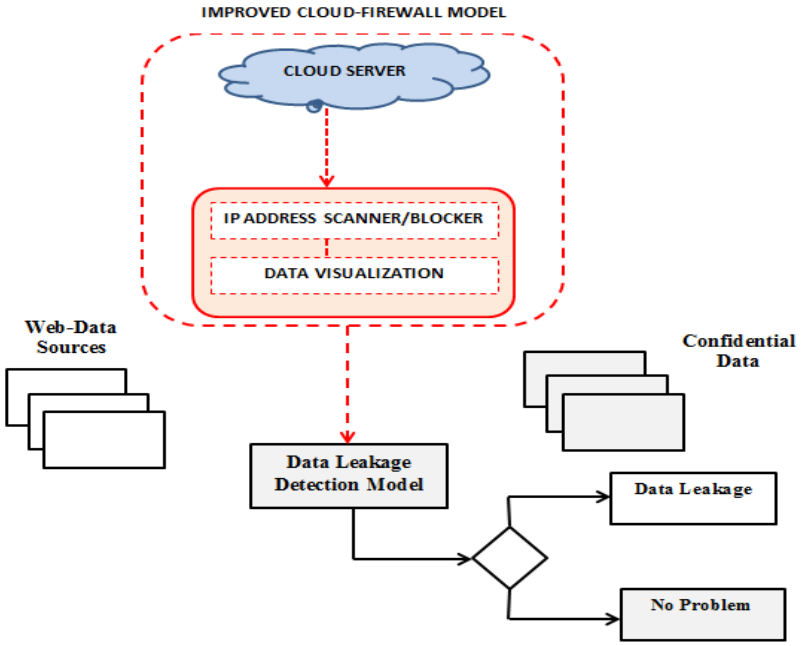

Fig. 3.2: Proposed System Architecture of an Improved Cloud-Firewall Model for Data Leakage Detection and Prevention on Email platform

3.3.1 Advantages of the Proposed System

The following advantages of the Proposed System are:

i) Provision of Security and Confidence to Email platform Users:

When Email platform users feel confident about their interactions with data that must follow security protocols, the less likely they are to cause an incident. Human error is after all the leading cause of breaches and attacks.

ii) Protection of organizational assets information on Email platform:

The ability of the proposed system to detect and block potential malicious data leakage will prevent guilty agents from stealing confidential information on organizational assets.

iii) Awareness on malicious and inadvertent data leakages on email platform:

A major benefit of the proposed system is the awareness on malicious and inadvertent data leakages problems to email platform users. This will also enable email platform users to carry out investigative measures on any suspicious advert that will perpetuate data leakage.

3.3.2 Existing System Algorithm

```
STEP 1: START
STEP 2: PUBLIC CLASS DLD (DATA LEAKAGE DETECTION {
   STEP 3: PUBLIC STATIC VOID MAIN(STRING[] ARGS){
      STEP 4: INT[] DLD = {3, 0, 0, 1, 0, 1, 3, 2, 0, 0, 0, 1, 2};
      STEP 5: SYSTEM.OUT.PRINTLN(FEATURES (DL)(DLD));
   }
   PUBLIC STATIC INT CONTA_ZERI_MAIN(INT[] V){
      IF (V.LENGTH == 0 || V.LENGTH == 1)
         RETURN 0;
      ELSE
         RETURN CONTA_ZERI(V, 1, V.LENGTH);
   }
   PUBLIC STATIC INT CONTA_ZERI(INT[] V, INT I, INT F){
      INT M,RESULT,SX,DX;
      IF (I >= F)
         RETURN 0;
ELSE{
         M = (I + F)/2;
         SX = CONTA_ZERI(V, I, M);
```

```
        DX = CONTA_ZERI(V, M+1, F);
        RESULT = SX + DLD;
        IF ((DLD[D] == V[M+1]) && (V[M] == 0))
          RESULT++;
        RETURN RESULT;
      }
    }
}
```

3.3.3 Proposed System Algorithm

STEP 1: START
STEP 1: INT MEMO[N+1]; // WE WILL INITIALIZE THE ELEMENTS FOR DLDP (DATA STEP 2: LEAKAGE DETECTION/PREVENTION TO -1 (-1 MEANS, NOT SOLVED IT YET)
STEP 3: INT GETMINSTEPS (INT N)
{
STEP 4: IF (DL == 1) RETURN 0; // BASE CASE
STEP 5: INITIALIZE DLDP
STEP 6: IF(MEMO[N] != -1) RETURN MEMO[N]; // WE HAVE SOLVED IT ALREADY :)
STEP 7: INT R = 1 + GETMINSTEPS(N - 1); // '-1' STEP . 'R' WILL CONTAIN THE
STEP 8: OPTIMAL ANSWER FINALLY
STEP 9: IF(N%2 == 0) R = MIN(R , 1 + GETMINSTEPS(N / 2)) ; // '/2' STEP
STEP 10: IF(N%3 == 0) R = MIN(R , 1 + GETMINSTEPS(N / 3)) ; // '/3' STEP
STEP 11: MEMO[N] = R ; // SAVE THE RESULT. IF YOU FORGET THIS STEP, THEN ITS STEP 12: SAME AS PLAIN RECURSION.
STEP 13: RETURN R;
}

IV. RESULTS AND DISCUSSION

4.1 Choice and Justification of Programming Language used

Hypertext Preprocessor (PHP) and MySQL were used in implementation as we shall briefly discuss them in order to shed more light on the discussed issue. PHP is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML.PHP code may be executed with a command line interface, embedded into HTML code, or it can be used in combination with various web template systems, web content management systems, and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in a web server or as a Common Gateway Interface executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP can be used for many programming tasks outside of the web context, such as standalone graphical applications. MySQL is the world's most popular open source database. With its proven performance, reliability and ease-of-use, MySQL has become the leading database choice for web-based applications, used by high profile web properties including Facebook, Twitter, YouTube, Yahoo! and many more. Oracle drives MySQL innovation, delivering new capabilities to power next generation web, cloud, mobile and embedded applications. MySQL has received positive reviews, and reviewers noticed it "performs extremely well in the average case"

4.2 Discussion of Results

From figure 4.1, the system user logs into the email platform. He or she inputs a unique username and password in order to select any of the platforms that involve Facebook, Twitter and Gmail. Each email platform link leads to their respective validation page. We perceive the importance of the system to Email platform users due to its vital role in the input of confidential datasets from the email platform users. Email platform is a new generation digital platform where the simultaneous sharing of web technologies is followed. This platform, consisting of items that facilitate and accelerate our lives and it is a collection of digital media and technology that allows users to share with each other, allowing users to create media content within individuals or groups. Email platform has become the most important information element of daily life. People are guiding and planning their lives through mass media. Figure 4.2 shows the login page of the email platform user, while figure 4.3 shows the Facebook environment with a fraudulent Access Bank link posted by a guilty agent. Figure 4.4 shows the input process of the unsuspecting user after clicking on the fraudulent Access Bank link. Figure 4.5 shows the pre-submission stage by the unsuspecting user. While figure 4.6 shows the data leakage and blockage alert by the system, which further creates awareness to the user.

Furthermore, the need for adequate classification of data security is highly indispensable. These security classifications reflect the urgency in handling of the classified information whether it is restricted, confidential, and secret or top secret in any cases. After all, there is also need for national data security. These measures should be taken seriously by email platform users, security agencies, and software developers, and data analysts. Another reason for this is that poor data security portrays a bad picture in data handling. Data security is assumed to be technological when there is an application of sophisticated security software, hardware, Cloud-Firewall, encryption methodology, network protection scheme or regular penetration test.

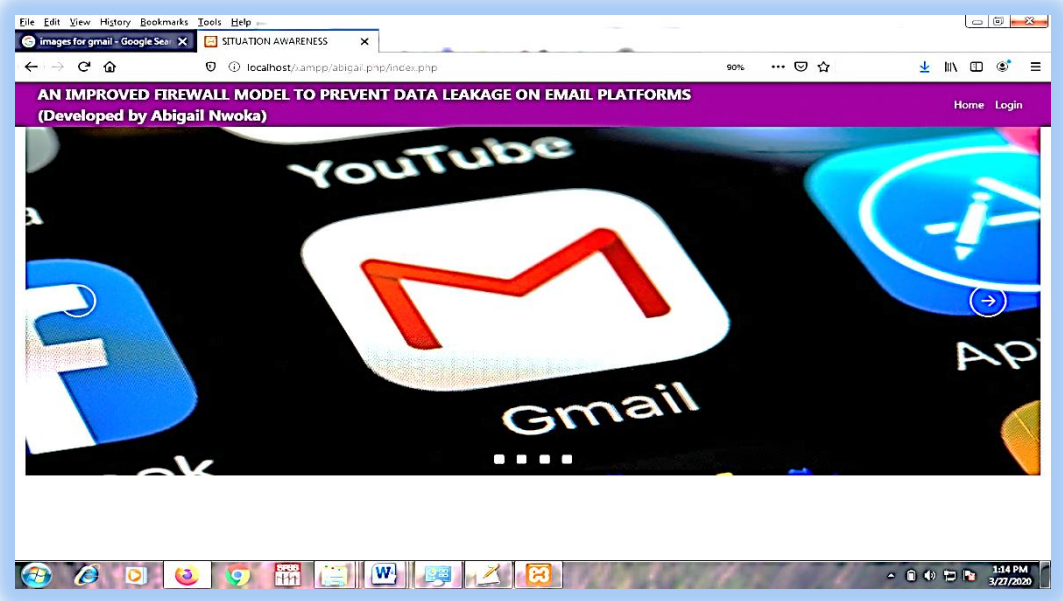

Fig. 4.1: Email platform: Welcome Screen

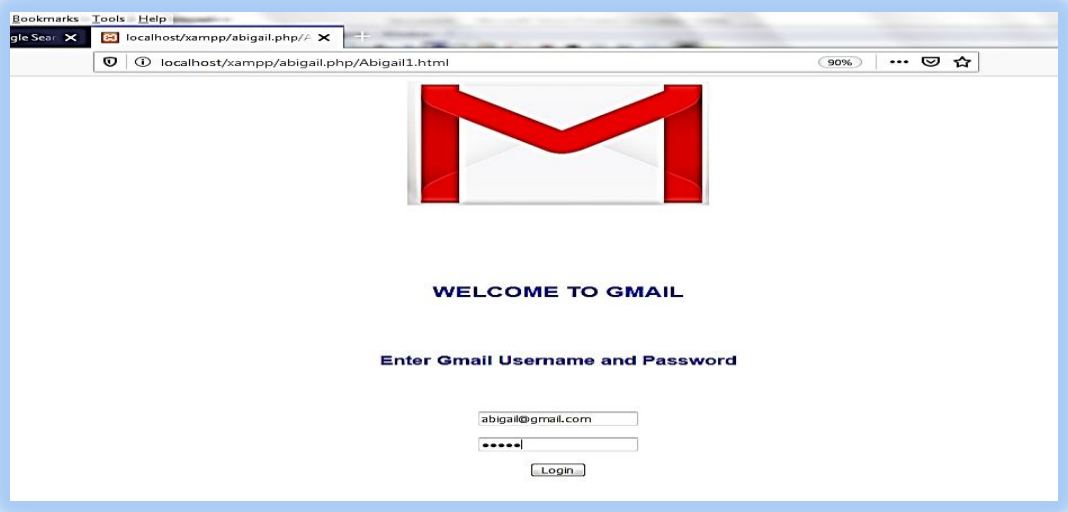

Fig. 4.2: Email platform: Gmail Login Page

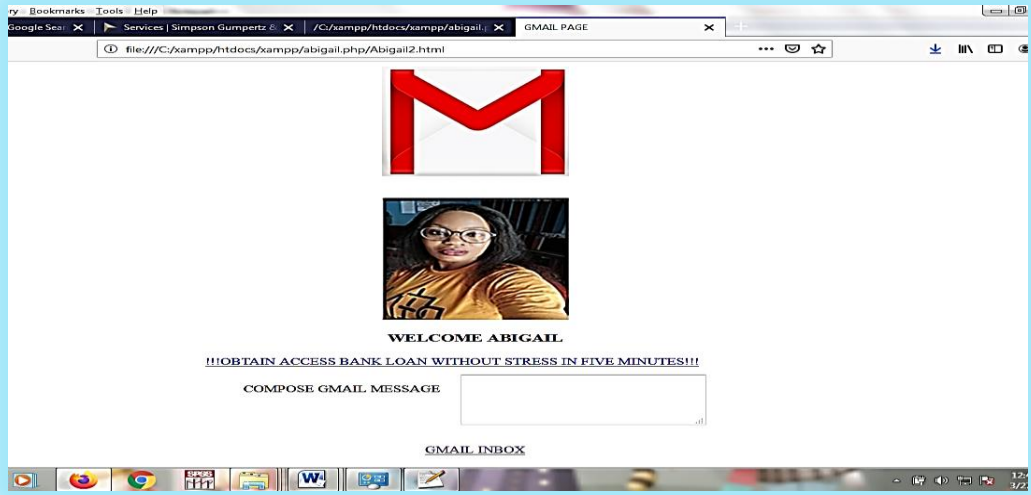

Fig. 4.3: Email platform: Facebook Environment

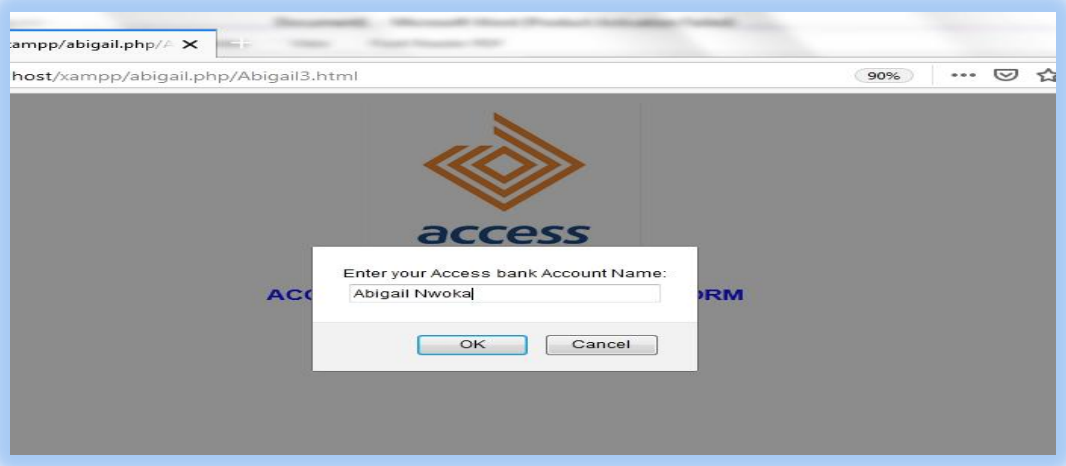

Fig. 4.4: Fraudulent Access Bank Form for Data Leakage

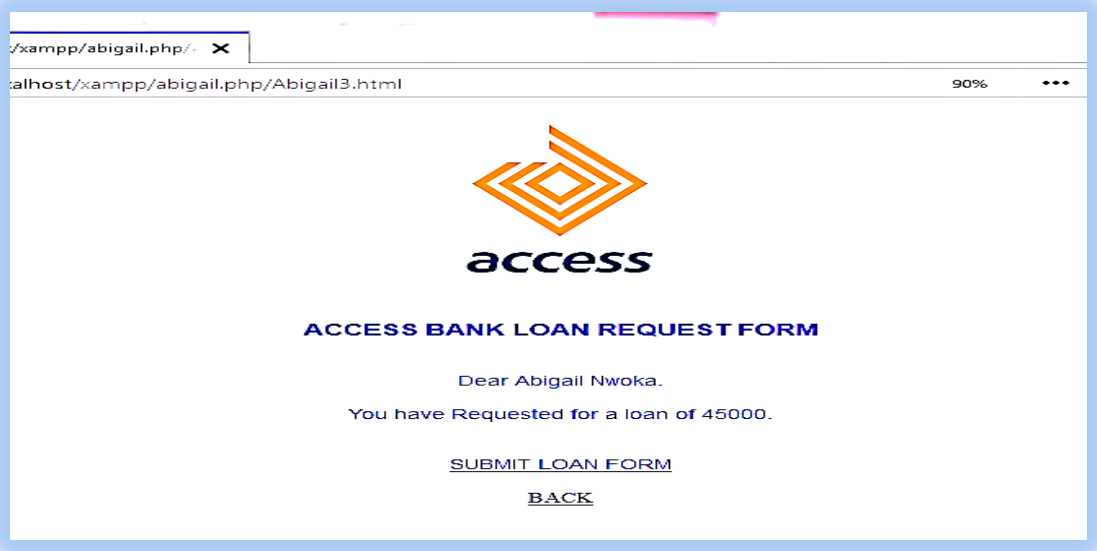

Fig. 4.5: Fraudulent Access Bank Form for Data Leakage (contd.)

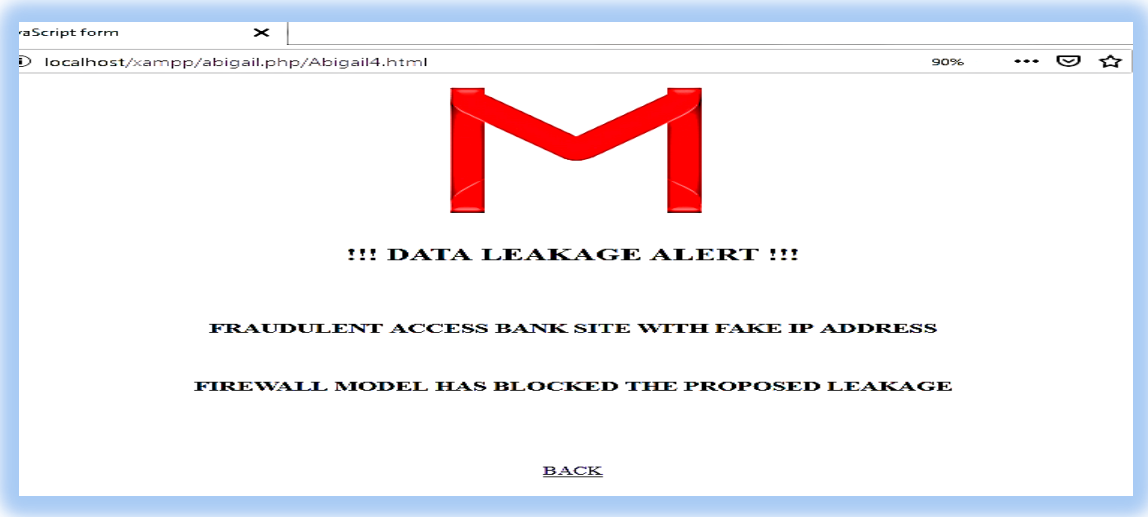

Fig. 4.6: Data Leakage Alert

4.2.1 Performance Evaluation of the Existing and Proposed Systems

Table 4.1: Comparative Analysis of the Existing and Proposed Systems

SN	EXISTING SYSTEM	Time in Seconds	Time in Seconds	PROPOSED SYSTEM
1.	Speed in Access Validation of Email platform users	37	19	Speed in Access Validation of Email platform users
2.	Speed in Data Leakage Detection	45	12	Speed in Data Leakage Detection

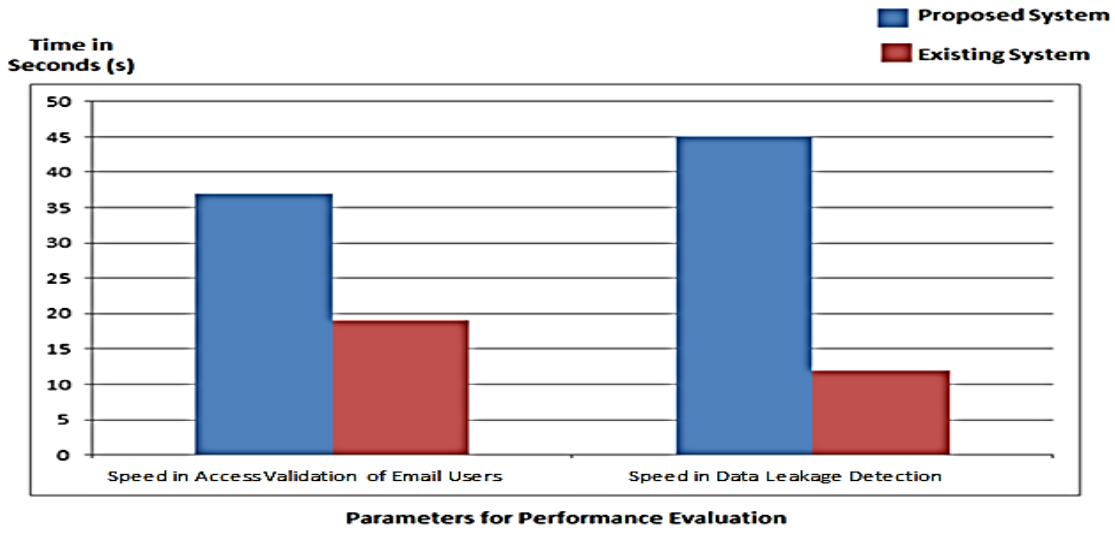

Fig. 4.7: Performance Evaluation Chart

V. CONCLUSION

In this study, we have developed an Improved Cloud-Firewall Model for Detecting and Preventing Data Leakage on Email platform. In addition, situation awareness on data leakage is very important to email platform users. This is because, not every email platform user takes data security seriously. A major challenge faced by most email platform users is the problem of data leakage. Two major data leakage problems include Malicious Data Leakage and Inadvertent Data Leakage. Most guilty agents that leaks data always utilize the ignorance of most email platform users that are desperate to release confidential datasets to unknown sources.

REFERENCES

[1]. Chadni. B.,Holls, O.,Anorld, L.: Data Leakage Detection, International Journal of Computer Science and Information Technology, 5(2), 2556 – 2558, (2016)

[2]. Archana, V.,Henrika, P., Abdul, S.: Data Leakage Detection, International Journal of Advanced Engineering Technology (IJAET), 3(1), 315 – 321, (2016)

[3]. Andrienn, S.: Data leak: Data Leakage Detection System: MACRO 2017 – 5th, International Conference on Recent Achievements in Mechatronics, Automation Computer Science and Robotics 6(4), 23 – 29, (2019)

[4]. Mica, R.: Towards a Theory of Situational Awareness in Dynamic Systems, Human Factors, TheJournal of the Human Factors and Ergonomics Society, 37(1), 32 – 64, (2015)

[5]. Prema, J.: Implementation of Data Leakage Detection using Agent Guilt Model, International Journal of Engineering research and Technology (IJERT), 2(1), 1 – 8, (2013)

[6]. Chirag, L.: Data Leakage, Detection and Prevention of Data Leakages in Web Servers, International Journal of Computer Science and Information Technology (IJCSIT), 5(2) 2556 – 2558, (2017)

[7]. Atif, D.: Information Leakage through Email Platforms; Opening the doorway for Advanced Persistence, Threats, Proceedings of the 8th Australian Information Security Management Conference,http://ro.ecu.edu.au/ism/93, (2016)

[8]. Krubhala, J.: Online Social Network: A Threat to Privacy and Security of Human Society, InternationalJournal of Scientific Research and Publications, 5(4), 1 – 6, (2014)

[9]. Mohammed, F.: Social Networks: Privacy Issues and Precautions, ICDS 2015: The Ninth InternationalConference on Digital Society, (2015)

[10]. Reddy, L., Libolsi, O., Gavin, H.: Data Leakage Using Cloud Computing, InternationalResearch Journal of Engineering of Engineering Technology (IRJET), 6(3), 6939 –6945, (2019).

Onuodu, Friday Eleonu, et. al. "An Improved Cloud-Firewall Model for Detecting and Preventing Data Leakage on Email Platforms." *American Journal of Engineering Research (AJER)*, vol. 9(05), 2020, pp. 71-81.