COVID 19 PANDEMIC: IMPACT ON BUSINESS AND CYBER SECURITY CHALLENGES

[1.]Dr. Archana Sharma , [2.] Purnima Gupta
[1.]Associate Professor, [2.] Assistant Professor,
[1]. IT Department, [2.] IT Department,
[1.] IMS Noida ,Noida, India [2].IMS Noida, Noida, India.

Abstract: The COVID-19 outbreak is a massive compassionate emergency that has also rigorously affected the worldwide economy. The rapid and unpredictably broad distraction to businesses around the world has left companies struggling to sustain security and business stability. As businesses/organizations have shifted to remote functioning to safeguard their employees while continuing to serve their customers. Companies have moved the majority of their actions to the digital world which leads to the high risk of cyber attacks. There are few challenges that how to secure this remote working practices while ensuring essential business functions are operating without any disruption and further how to keep the organization protected from attackers by taking the advantage of the uncertainty of the situation. The research explores the current trends of cyber security threats during the pandemic and further highlights the impact of COVID -19 on global business environment and the various types of cyber security challenges have to face by business leaders and the individuals with the preventions may be taken organizations to protect the business from the security breaches.

Index Terms: **Phishing Attack, ransomware, maze, corona virus, emotet, trickbot, EDR.**

I. INTRODUCTION

Pandemic which has been really considered as a worldwide cyber pandemic initiated 20 years ago. Till date, cyber crimes have expended exponentially and multiplied to every place of across the globe. A person's data is expected to be infected online by physical existence in either any area like Southeast Asia, eastern Europe or Africa. This global cyber epidemic has been accelerated speedily by states. Over the past 20 years, cyber capabilities have frightening new mechanism of national power. The COVID-19 pandemic has altered the way business is done around the world. With mostly remote personnel operating on unsecured networks at home, business security players are struggling to control of speedily growing attack areas. Cybercriminals along with the state-sponsored highly developed threat groups take advantage of the COVID-19 pandemic for attacking the networks across the world to get the benefit of monetary and the intentional gain. Between January and March 2020, corona virus-themed phishing allure, various malware contamination, network infringement, rip-off, and disinformation battles have become uncontrolled across the clear, profound, and murky web. This research to explore the most prevalent COVID-19 cyber threats: phishing websites and emails, fake corona virus mobile apps, malware, ransomware, fraud, and disinformation. It also addresses the criminal and state-sponsored threat actors behind these campaigns, the most common types of targets, and network indicators of compromise.

The FBI look forward to cyber player with the excessive use of virtual environments by various government sectors, the private organizations and individuals due to the impact of COVID-19 pandemic[1]. As Computer systems, Smart phones and virtual environments endow with necessary communication services for remote work and education, in addition to carry out normal business. Cyber players take advantage of vulnerabilities in these functional systems for unauthorized access and lift the sensitive or confidential information, target the individuals involved in passing data over network and financial transactions performed by industries. A threat of troublesome and destructive attacks have been targeted to organizations across industries and geographies by various targeted ransomware incidents.

Initiation with simple phishing attacks and hand sanitizer scams now several predictable threat player have become more active in COVID 19. APT36, FIN7, the Maze ransomware group, and several other country state players are now at the back attacks related to the coronavirus pandemic. As sophisticated threat players enter this loop, both the volume and sophistication of the cyber attacks will probable increase in future.
The research suggests the following steps for resistance against these threats:

- Update the present threat countryside risk measurement based on new budding threats to remote workforce.
- Intimately supervise collaboration and remote working platform.
- Stringently enforce the use of VPNs, security measures like encryption and endpoint security also.
- Impose strong password policy and two factor authentication.
- Educate the employees and individuals on the new cyber threat landscape.

II. SECURING THE NEW REALITY IN COVID 19

There is a transformation in work of individuals due to COVID and enforced the way organization working culture, the completion of projects which might have been of about a year duration now have been motivated to finish within weeks. Practicality has been considered as a rule, with the acceptance of this reality , business organizations have taken the various cyber security risks also which might never have established in other situations. Structured cyber crime clusters have shown themselves merciless and

industrial in taking advantage of fear, uncertainty and uncertainty over COVID-19 —deliberately phishing and attack communications to build out COVID-19 forged websites and evade. States themselves have personalized their own cyber surveillance strategies.

The impact of COVID-19 on the universal cyber security marketplace is expected to raise from USD 183.2 billion in 2019 to USD 230.0 billion by 2021, at a Compound Annual Growth Rate (CAGR) of 12.0% during the estimated time. The marketplace expansion can be accredited to upward focus on securing remote communications or infrastructure and IP of organizations due to work from home and various remote service activities and schedules. For all businesses, the key focal point should be on cyber security instead of just as a sustain function to drive the marketplace with a higher holder share for cyber security guidelines and infrastructure.

2.1 Different types of Cyber Attacks Active in Pandemic COVID 19

Cyber security is really becoming a apprehension for organisations that how to sustain the security of data and adopt the new working culture in this changed world after observing the rage of Corona pandemic. This amplified remote working cultures has now made business enterprises with higher vulnerability for Cyber threats and attacks. Thus to overcome with this situation, IT professionals of all kind of enterprises and start-ups are now drawing some additional cyber security policies for the to improvement of their IT infrastructure.

2.1.1 Phishing Attacks

Most of the companies and organizations of private sectors practicing this change in their working culture lately just because of COVID-19 pandemic. Remote activities like tele working are increased .It is mainly reliant on E-mail for message communication, which leads to email fraudulence activities [3].

Cyber criminals are captivating benefit of the COVID pandemic by spreading the awareness of the Corona as subject to dodge users into enlightening their personal details or clicking on malevolent attachment or links, unintentionally downloading malware to their systems[4]. These security breaches may even pretend to be with any public or private sectors, health ministries, or any reliable sources or figures in any country. Such emails seems to be authentic including logos or brand name of the particular organisations. According to Barracuda Networks , a foremost provider of cloud-enabled security and data protection solutions report[5], the diversified phishing movement are taking benefit of the susceptible centre of attention on COVID-19 to share out malware, whip credentials, and cheat users out of money.

The general phishing strategies have been observed for such cyber attacks. Moreover a large number of movements are using the corona virus to attract and use a trick for unfocused users to take the benefit of the fear and uncertainty of their projected victims. During March 1 to March 23, the research detected 467,825 email and phishing cases, out of them 9,116 were associated with to COVID pandemic [6]. The figure 1 shows the analysis of emails sent during Jan. 2020 to May 2020 related with the COVID-19 threats.

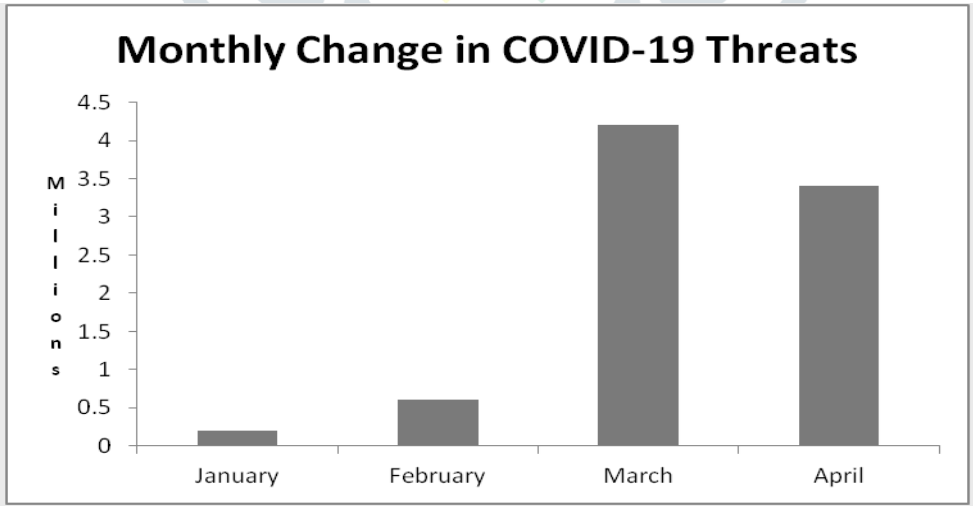

Figure 1: Analysis of 1 billion emails sent between 1 Jan., 2020 – 1 May, 2020

"All COVID emails does not include emails referencing Coronavirus/COVID-19 in the email body but not in subject area"

While analyzing the threats, it has been observed that malicious groups generally trust on masquerade tricks like "official" communication through HR representative or executive or create the URLs like WHO, CDC etc. looking for the credentials or confidential information or financial details. Most of the time COVID -19 have been used by cyber criminals to build ransomware and threat of phishing.

2.1.2 Malicious domains

For malicious activities over internet related with COVID-19, cyber criminals registered various domains containing the terms like corona-virus, coronavirus, covid-19 and covid19.Although, there may some legitimate websites also. For masquerade and spam drives, cyber criminals create thousand numbers of new websites regularly. By taking the benefit of worldwide communication on COVID pandemic, cyber criminals embed the Malware, Trojan and Spyware in interactive corona websites and maps of corona virus.

2.1.2.1 Remcos RAT Malware

An executable file "CoronaVirusSafetyMeasures_pdf[.]exe."[7] is dropped as unidentified contamination vector to spread the Remcos RAT malware. It persist during the start up key to permit the malware to restart and installs a Remote Access Trojan as the victim start the system again and malware logs the individual's keystrokes and command IP. Due to COVID -19 spam cases have been increased in large number and threaten with COVID -19 in failing to pay a ransom amount. The demand of ransom in bitcoin as $500 or threat of corona virus in next 72 hours and the emails come into sight to be sent from the victim's legitimate account. In most of the cases the IP addresses are of East Asia[7]. Seqrite, a cyber expert on May 18 reported that to target the specific Co-operative banks in India, a unknown corona virus based emails were claimed to be from Reserve Bank of India.

2.1.2.2 Lokibot

To lift the data and email credentials like user id and passwords to FTP server and crypto coin wallets, a another kind of malware Lokibot has been activated and distributed in unlike corona pandemic related phishing movements.

The FortiGuard Labs of Fortinet, a security firm released a report and revealed that the spear-phishing movement is spreading the Lokibot , a email credential stealer by taking the benefit of fear of COVID -19[8]. Spear phishing emails are generated in English with abundant grammar and lots of spelling mistakes. The report further highlights that once the attachment file is opened and decompressed , a another file with the name"DOC.pdf.exe" displayed and if it opened, this file projects the Lokibot within the infected system.

2.1.2.3 Trickbot

Trickbot initially treated as a Trajan for banking, but now it has been re-treated as one of the advanced and proficient form of malware spreading around the world. Since the starting of the year 2020, the check points at various location has found at most, 4000 COVID-19 associated registered domains globally whereas 13% of them were initiated as malicious and 5% in addition to found suspicious and investigated[9]. It has been observed that Covid –connected domains malicious rate is increasing speedily

2.1.2.4 Emotet

Emotet permits cyber attacker to steal confidential details or money of victim's computer system or mobile device as infected by it. In this pandemic situation, Emotet spreading the cyber scams as it is self propagating malware and being used as dropper to dispense ransomware and other malware which will take the hold of the targeted system for stealing the confidential information, execute the crypto jacking fiddle or may catch it for ransom[10].

As a Trojan, Emotet is initially spread through malspam mails which may enter to the victim's system through various ways. It may be malicious link, malevolent script, document file with macro. Emotet infected emails may associate similar branding design seems to be the legitimate mail. It may also persuade the end users to click the infected files with the use of attractive language like Payment Details, Invoice Details etc[11]. Emotet is very difficult to identify as it applies indescribable techniques to evade detection, as dynamic link libraries. The one of the case of phishing movement was to target the Healthcare on 22 April, 2020 Emotet Botnet which shows the Signs of Life & COVID-19. It has been concluded by DHS that this Emotet malware is one in the majority of destructive and costly malware which spreading the infection in all types of organization as public or private, government, individual and costing very high to clean up as $1 million per confrontation[12].

2.1.2.5 Formbook

Formbook malware with the data stealing capability from the web browsers and number of other applications also. In a research of malicious attacks of COVID –related campaigns, both Trickbot and Formbook attacks have been seen in a large number, specially in May, 2020[11]. An email movement pretending to be the information about the corona virus latest updates from WHO(World Health Organiation) is spreading a malware downloader to install the Formbook Trojan to steal the information. This email also contains a attachment as ZIP file with a statement from "World Health Organization" and the ZIP file contains the "MY-HEALTH.PDF" which was attaché for the phishing purpose only. Although it will pretend to user about the latest update about the corona virus statewise. The formbook malware as downloaded to the system put efforts to steal the contents of log, Windows clipboard, keystrokes and web browsing data.

2.1.2.6 Ransomware

Another type of malware, ransomware usually encrypts the data and blocks the accessing of computer system and demand the payment to pay to the attacker with deadline sometimes. In case of no payment in time, the data may be lost forever. Different kind of organizations, consumers, hospitals, public institutions, medical centres and industries are being under attack by ransomware. Due to health disaster they are not in position to locked out their computers ensures the cybercriminals that victims are interested to pay the amount demanded. Sophos, a security firm revealed the analysis on ransomware attacks in May, 2020 including the 5000 IT managers accorss the globe. It was observed that more than 50 percents of the surveyed organizations were attacked by ransomware[12]. In U.S, the estimated ransomware cost of year 20202 could be approx $1.4billion. This number could be increased by adding the cost of downtime and revival by $9 billion in 2020. Approx. $111000 was the average amount of ransomware attack on enterprises in Q1 of year 2020 and $40,000 was average ransom imbursement[13].

2.1.2.7 Maze Ransomware

The Maze ransomware generally hits the organizations and companies by infecting the corporate network and computers with windows os. It encrypts the data and block to unable the accessing by end user for ransom demand. As the COVID-19 is being speed up across the world , the maze ransomware attacks has also increased in various IT companies like Cognizant, Conduent etc. The foremost feature of this malware is that malware creator threaten to the victims for ransom payment otherwise the information would be released over open network. Initially some cyber criminals had promised to not consider the medical services during this pandemic, but few didn't agreed for it . Maze attacked the US Law companies, German administration, HMR company. HMR company carry out the clinical test and prepare the vaccines for corona virus. On 14th March, 2020 , this company was attacked for 2,300 patient medical records and on 21st March, 2020, employees details were leaked.[14].

2.1.2.8 NetWalker Ransomware

Mailto malicious software (Net Walker Ransomware) was revealed by GrujaRS and restructured version of Kokoklock malware. The main feature of mailto malware is to encrypt the files and reproduce them by renaming them to make unusable for victim with the creator's mail address and victim's distinctive ID as extension[15]. The Netwalker group are not hesitating to exploit the COVID -19 outbreak by infecting the computers of the individuals and entities who are involved in health organizations or health service industry. The disillusioned emails sent by this malicious group masquerade themselves to represent associated with corona virus disaster but as the recipient click on the attachment file of Excel or Word file, their systems get infected.

With the subject corona virus, phishing mails were sent with the malevolent attachment with the name "CORONAVIRUS_COVID-19.vbs" which contained the embedded NetWalker malware execulable file in starting of March, 2020 to various organizations[16]

2.1.2.9 Extortion and Fear Tactics Through Ransomware

The conventional cyber-criminal groups are still sustained with the art of theft of credit cards and individual information for a simpler approach called cyber extortion. Under this, Victim's money is demanded instead of stealing it. Cyber extortion persist to put on grip just owing to millions of dollar criminal business. Regardless of law enforcement of governments and healthcare industries, could not run away of its conduit[17]. The cyber attackers are taking benefit of people's fright just about the COVID-19 for ransom money.

2.1.3 Palo Alto Networks Tracks Cloud Threat Landscape

The researchers have found 1.2 million domain names registered with the keyword associated with the name COVID-19 of Palo Alto Network of Unit 42 during 9th March to 26th April, 2020. It was found that approx 86,600 of the briefed domains are malicious. The highest figure of malicious domain in United States (29,007) with the trail of Italy i.e 2,877, Germany -2,564, Russia as 2,456[18].

End point security and unremitting threat scrutinize products are being sold by security retailers as well as PaloAlto Networks to prevent employees automatically as they visit such type of malicious domains. In addition to these security instruments, it has been observed that employee education regarding cloud based threatening also required as unknown file click could be a malicious movement[19]

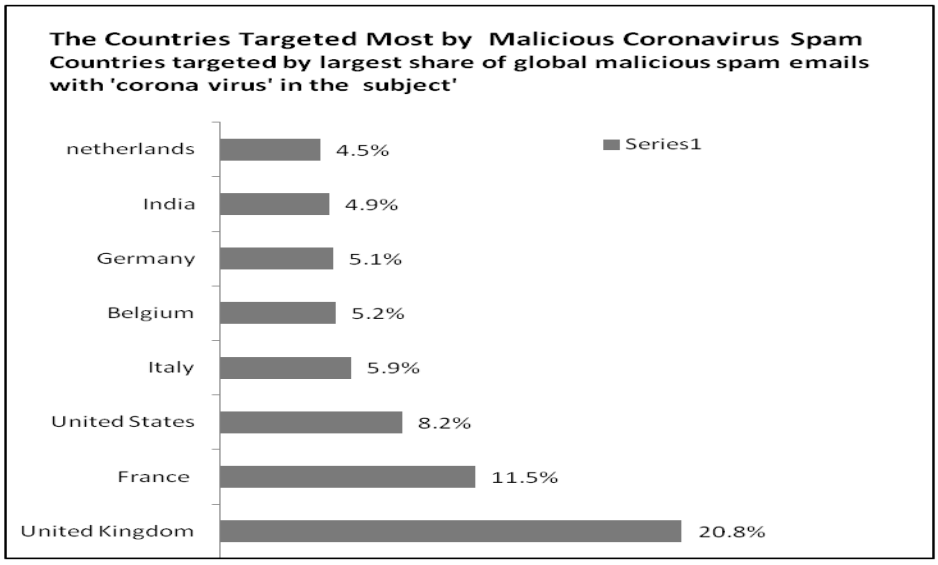

Figure 2: Malicious Coronavirus Spam (January 1 to March 27, 2020, Source Trend Micro)

III. CYBER SECURITY THREATS TO INDIVIDUAL AND BUSINESS ORGANIZATION

Unfortunately fraudsters have a tendency to wish on unpredicted challenges or events. Due to disruption of normality they look for an opportunity which may exploited. Fraudulent activities have significantly increased due COVID-19 pandemic. For most of the people life have become very tedious and unusual and more at risk while work from home, financial crisis, future prospects etc. Retailers and other businesses are also facing significant uncertainties over cash transactions and revenues, international trades.

3.1 Individual and Private Banking Customers

The private and individual banking customers are natural aim for cyber criminals. It has been observed that the 'phishing' cases associated with COVID-19 increased, the emails seems to be from bank for financial help available due to pandemic, but unfortunately these mails may contain suspected malware that are downloaded onto the customer's computer once clicked the link. Call centres frauds are also increased. Proactive actions of bank are making the customer aware about the security of the system and guiding them about the phishing attacks.

3.2 Challenges of employee remote connection

However, Banks are not only concerned and strive hard for customers to protect from cyber criminals, the risk has increased for staff also. It may be just because of unintentional consequences of bulk movement of employees to work from home that cyber criminals have become more active and phishing mails and scams have been increased. At the same duration most of the working family members share the same network while doing their official work and download the contents with click invites the malware at their system and could take entry in the firm also if the end point security is proper. The eavesdropping or take control of the conversation in case of video conferencing also has been increased in this pandemic time.

3.3 Trader surveillance intermittent

Trading is the another area where surveillance is required and monitoring as well as recording of also required as per the regulatory guidelines. The other area of surveillance is Trade. According to the regulatory rules, the recording and monitoring of traders call are essential. Unfortunately, now Tader's calls are unrecorded due work from home and pandemic situtuation.

The impact of Corona virus on Trade in India have estimated approx 348 million dollars, according to United Nations report, in addition to it the country has been counted among major 15 financial market which have affected due to china's manufacturing process slowdown as disorder of china international trade[20].

3.4 Healthcare Sector Challenges

In COVID-19 pandemic situation, as all hospitals, health care workers, doctors and staff looking after the patients while in other side of the world, the cyber criminals are looking for the exploitation of this pandemic outbreak[21]. The healthcare segment have been facing the new challenges in COVID-19 pandemic due to strong data integration and IT infrastructure. Although it is positive but invites the network vulnerable to various types cyber attacks like, ransomeware, email phishing, network data breaches due IT as a backbone of healthcare sector now a days. The major target areas are Laboratory management system, Hospital record system, Individual health record, radiology information system and email servers. The cyber criminals also focus on endpoint devices which involves the patient monitoring kit that are generally connected to the internet.

3.5 Manufacturing Industry Challenges

Supply chain security has major issue of cyber threats globally in COVID-19 outbreak. The supply chain integral process mainly dependent on data process by suppliers or services provided them. Due to corona virus and related global lockdown, the drastic risk of short and long term have been causing in companies supply chain process. The cyber security risk have been increased at present due to organizations trust on most of the suppliers with confidential and sensitive data[22].

The research highlights the other key aspects to be focused by suppliers that :

Multi factor authentication has not been enforced while remote access of services, No formal agreements have been put by some of suppliers to restrict the third-party deployment of data, No data security training is being provided to the some supplier's employees, lack of penetration tests of IT infrastructure which are directly connected with public.

IV. CYBER SECURITY BREACHES PREVENTION TECHNIQUES FOR BUSINESS ORGANIZATIONS

To prevent the business organizations from cyber security breaches, Endpoint security is must as a solution which includes the Endpoint Protection along with Endpoint Detection as well as Response solution. These two solutions together secure the remote devices employed in organizations and endpoints from various malwares, Trojans as well as other unknown advanced threats. Endpoint Detection as well as Response solutions allow unremitting detection and quick response in case of any unknown cyber security threats and monitoring of cyber security.

In case of major workforce of organization working remotely, there is a need to focus of data privacy and cyber security mainly on the below mentioned four areas which are generally to vulnerable to a breach are This may support to ease the breach happening in reality and restrict any possible liability.

There are four major areas has been highlighted to remain the business secure from cyber criminals and data violation during the noisy time.

4.1 Email Security

It is very much essential to know for all individuals about the email security. Most of the attacks are happened through email only in this COVID-19 pandemic. The person should avoid to open the suspicious or unknown emails, downloading the unexpected attachments. Verification of suspicious attachments or links is required before open it through any other mode of communicati on like text message. Never provide the personal details to unknown suspicious resource like birthdate, password or social security number. Be aware with emails of poor grammar or poor design as it can be a phishing attack.

4.2 Password Protection and Multi-Factor Authentication

Always strong password should be set on all employee's and individual's account. All individuals should avoid password which may be easily identified like birtdate, pet name, spouse name etc. Such password are attempt of Brut Force attack.

4.3 Web Safety

As the research highlighted, in this COVID-19 pandemic massive invasion of bogus websites, whose developers are looking for the opportunities by taking the benefit of fear in nearby of coronavirus. Always ensure that any site looking for require the account personal details like username and password. In case of financial transaction, a valid encrypted digital certificate is associated to ensure the data security. Secure websites always begin with "https". Remote workforce should avoid the public systems and Wi-Fi connectivity for accessing the confidential information. Always sign out all accounts and shut down the device either computer or mobile device when it is not functional.

4.5 Device Maintenance

As various cyber criminal groups are active during COVID-19 outbreak, thus there is a need to keep all resources like hardware, software etc updated with latest versions. All Employees should take the regular backups with multiple copies of all important and critical data and keep safe away from the network from the ransomware attack or unknown malware attacks. Such kind of prevention will allow to maintain the data protected from malware attacks. There must be cyber insurance policy of the organization.

4.5.1 Identify supply chain risk

A supply chain build up with various activities in manufacturing process which includes the transformation of usual resources, material in raw form and components finally into a complete or finished good that is to be transport to the customer. Thus in this CONID-19 situation, Business need to identify the loose end points while workforce working remotely. When any link within supply chain process fails, the entire business process disrupted. The post effects of it may be in inflation of costs, reduced revenues, reduce customer assurance, market share down.

V. RESHAPING THE BUSINESS MODEL AS CYBER SECURITY SOLUTION

As the demand of the current scenario during COVID -19 outbreak to reshape the functionality of the organizations in an innovative way with the mixture of work from home and office of the employees. To communicate and access data remotely over email, strong network connectivity is required. Additional dynamic authentication need to added as cyber security solution. The additional Cloud security alternatives is essential. Few organizations under COVID -19 cyber attacks now come up to re-examine the detection of cyber security infringe and scam control algorithms, modernize the IT infrastructure for the revised hybrid functional models.

There are some learning around flexibility from COVID-19. The current situation of corna virus enforced the organizations to reshape their business models todeal with hybrid functionality of workforce, maintenance of customer demand and fulfilment at supplier end. Companies have been forced to create and mange crisis management alternatives and handle it with pace. All individuals should learn these matter to face all kind of situations.

CONCLUSION

The protection of business as well as individual counter to cybercrime in the situation of COVID 19 and economy will be a top-down practice in this situation where the government leading role is required. Earlier, the Cyber threat was considered as the state tools and has vision cybercrime just for threat in case of only its engagement in espionage. Complicated security breach that wring individual person and different service providers like public or private has diminished between the gash in law enforcement retorts. This unresponsiveness is not conscionable more due to the exponential growth of ransomware with the support of cyber hackers to attack the various healthcare systems at the critical time of Corona outbreak. This research focused on cyber security challenges during the COVID -19 pandemic situation and various types malware and ransomware active to threat the business organizations and individual for their confidential information spread over internet. There is a need to measure the incidents and responses in addition to anticipatory measures. As the research highlighted the few measures may be considered by business, various industries, trade, banks and other private sectors and individuals as number of remote workers have increased due to corona pandemic and reform the business model as the safety measure.

REFERENCES

[1] www.fbi.gov/contact-us/field
[2] Covid-19 Impact on Cyber Security Market _ Coronavirus Outbreak & Cyber Security Industry _ MarketsandMarkets.html
[3] Covid-19 ignites a firestorm of cyber attacks
[4] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[5] https://ciso.economictimes.indiatimes.com/news/covid-19-related-phishing-attacks-up-by-667-report/74839322
[6] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[7]https://enterprisetalk.com/coronavirus-crisis/ibm-x-force-study-coronavirus-themed-spam-records-14000-spike/
[8] https://www.bankinfosecurity.com/spear-phishing-campaign-uses-covid-19-to-spread-lokibot-a-14058
[9]https://www.zdnet.com/article/trickbot-malware-is-using-these-unique-macro-laced-document-attachments-with-a-coronavirus-theme/
[10]https://www.livemint.com/technology/tech-news/phishing-scams-on-the-rise-amid-panic-over-covid-19-11583424287780.html
[11] https://www.malwarebytes.com/emotet/
[12]https://www.willistowerswatson.com/en-IN/Insights/2020/04/keeping-vigilant-against-increasing-cyber-risk-during-Covid-19-crisis
[13] https://securityboulevard.com/2020/05/covid-19-uncertainties-fuel-ransomware-attacks-and-phishing-schemes/
[14] https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/
[15]https://www.incibe-cert.es/en/blog/netwalker-ransomware-analysis-and-preventative-measures
[16]https://www.tripwire.com/state-of-security/featured/netwalker-ransomware-what-need-know/
[17] https://www.cisecurity.org/blog/cyber-extortion-an-industry-hot-topic/
[18] https://unit42.paloaltonetworks.com/covid-19-cloud-threat-landscape/
[19]https://www.sdxcentral.com/articles/news/mcafee-crowdstrike-palo-alto-networks-track-evolving-covid-19-cyberattacks/2020/05/
[20] https://economictimes.indiatimes.com/news/economy/foreign-trade/trade-impact-of-coronavirus-epidemic-for-india-estimated-at-348-million-dollars-un-report/articleshow/74487020.cms?from=mdr
[21] https://www.aha.org/news/blog/2020-03-19-four-ways-mitigate-covid-19-cyber-risks
[22] https://www.cpomagazine.com/cyber-security/supply-chain-security-on-thin-ice-in-the-age-of-covid-19/

Electronic Health Record (EHR) Security Based on Data Classification Using Machine Learning

Deepak Kumar Verma, IEC College of Engineering and Technology, Greater Noida, Uttar Pradesh, India.

E-mail: deepak.verma1980@gmail.com

Rajesh Kumar Tyagi, Krishna Institute of Engineering and Technology, Ghaziabad, Uttar Pradesh, India.

E-mail: profrajeshkumartyagi@gmail.com

Purnima Gupta, Dr.K.N. Modi Institute of Engineering & Technology, Modinagar, Uttar Pradesh, India.

E-mail: purnimaa018@gmail.com

Abstract--- The existing security mechanisms in EHR systems are based on common algorithms to secure patient's health data. However, every record of patients is not sensitive thus does not require same security. In this paper, we offered a new methodology to safeguard Electronic Health Records (EHRs) that first categorizes the patient's data into different security levels. Thus, we can reduce the time complexity in terms of encryption time and data uploading time on the cloud server. Firstly, the EHR of patients have been classified into three categories, namely high-sensitive, moderate sensitive and non-sensitive using a data classification approach of Machine Learning. Next, the classified data has been encrypted based on its sensitiveness with the help of appropriate encryption techniques. We have analyzed different security algorithms based on parameters like the time of encryption or decryption and the speed of generating the key which helps in reducing time complexity. The experiment result shows the effectiveness of the proposed methodology that can be used in future EHRs architecture.

Keywords--- Data Classification, Security, Cloud Computing, Electronic Health Record, Access Control.

I. Introduction

In order to expand the worth of health care, Electronic health record is the preeminent methodology to retain the patient's health records. EHR is a database of patient's medicinal particulars in digital presentation. When equated to the paper records this mode has numerous benefits. Ozair, Jamshed & Aggarwal (2015) stated that Electronic Health record aids us to preserve enormous amount of records and it is calm to increase all features of patient care, including proficiency, instantaneous updating of histories with correctness. We have taken the assumption for a cloud that provides services is semi-trusted and may temper the sensitive data of a patient.

These days EHRs are extensively used for storing patient's health data on cloud. The security of these systems needs more attention for the sensitive health data of patients. Cloud computing is playing an emergent role to splendid power on healthcare industry. Electronic Health Record consists of medical history of a patient like lab tests, e-prescription and images like MRI, X-Ray etc. Martinez, Sanchez & Valls (2013) proposed a security model for protecting outsourced health data of a patient from the curious and malicious cloud service providers. The patient's health data is stored on cloud servers openly or using encryption of complete data. As the data have diverse features, so it needs different security levels according to the necessity. Therefore, security of patient's sensitive data can be provided based on the level. We cannot put all the data at the same level of security. There should be a mechanism that secures data effectively to reduce the complexity.

Classifying the data is a procedure of describing various levels of data and determining the sensitivity at various steps to it Saikh & Sasikumar (2015). The classification of the data determines the level to which the data necessities to be protected and its cost in terms of patient's data. Data classification is completed based on the risk associated with the disclosure. Classification of patient's data grounded on security level standards is fetching an area of attention by numerous officialdoms using cloud services.

We classified the patient's health data based on its sensitivity into three levels.

Received: 20 October 2018/Accepted: 15 November 2018

1. Restricted or high level: Most sensitive data having great risk if compromised. Access is on need-to-know basis only.
2. Confidential or medium level: it contains moderately sensitive attributes.
3. Public or low level: This is non-sensitive data. Access is loosely.

The dynamic level security mechanism based on data classification has received much attention in the current scenario. However, most of the security mechanisms use static level security and do not provide a systematic way to vary the level of security. From the study, we understand that there should not be common algorithms to process the whole data.

For security of the health data, we have to categorize the patient's data into different levels based on data sensitivity. So, we can reduce the effort and period of encryption as the data on the cloud server have diverse features and desires diverse security levels. The dynamic level security is moderately new and of scrupulous attention in the present scenario.

To the preeminent of our information, there is no prior effort that addresses leveled security problem. The key offerings of the work are along these lines.

1. We are proposing an overall architecture for EHRs that will automatically categorize the patient's health data into multiple levels using document classification.
2. Based on sensitivity of data, we are proposing different encryption algorithms along with their key combinations to secure EHRs at various levels.
3. We present a detailed analysis of the proposed approach on various encryption standards.

We have reviewed the existing encryption algorithms and have a comparison based on different parameters. We can allocate several security levels to the classified data by using various security models for confidentiality of patient's data. This will save our period of encryption and uploading of patient's data on server. It also avoids the data seepage so the adversary will not be able to identify the beginning and termination point of data. The determination of data classification is to create a context for categorizing data based on its sensitivity level and as per the requisite of the Organization's Information Security Policy. More encryption is anticipated for robust security however it needs additional computation. So a standard offers stability for the security and encryption overhead. We assume patient's confidential data is stored in semi-trusted cloud service providers. Ciphertext policy attribute based encryption (CP-ABE) is used for encrypting patient's health record to accomplish fine-grained access control. The respites of this paper are following. In Section II, the work correlated to data classification along with security is given in brief. In Section III, data classification and security framework is proposed, followed by methodology and the analysis performed through experiments in Section IV. The conclusion is lastly specified in Section V.

II. Related Work

Amato et.al. (2010) put forward a technology for semantics which can identify the associated security level of medical records to perform resource classification to ensure proper security rules to be applied. This methodology cannot be structured a-posteriori and is helpful to overcome the security issues when patient data is made available to new potential applications. Bollineni & Neupane (2011) concluded that cloud computing and its services provided by vendors, are getting less trusted among cloud users due to lack of knowledge about them. Data security and data integrity are the primary concerns for the people because of the complete dependency on cloud service providers. Mohamed, Abdelkader & Etriby (2012) advised different encryption algorithms depending on the different types of security level requirements. Users can follow AES encryption algorithm for highest security and DES or Blowfish can be used for better performance. Fernandez-Aleman et.al. (2013) concluded that an efficient encryption scheme is required for EHRs that are new and includes the less keys and its number at each step. RBAC is a scheme which incorporates digital signature based on PKI and login/password, and advised as the preferred authentication mechanism. Ghazvini & Shukur (2013) explored and analyzed the current e-health system for the security at the policy level to protect patient's health records and found that electronic patient record is mostly appropriate for healthcare organizations. Fakhar & Shibli (2013) discussed about different frameworks for cloud security mechanisms and trust management. Recent cloud security models are missing an approach for storage support of keys and creating central entities downgrades the performance of the services.

Shaikh & Sasikumar (2015) proposed a classification scheme for the data to provide security levels based on a set of their identified parameters. They classified the contents before storing them to cloud and allowed this provision for message encryption and access control tools.

Received: 20 October 2018/Accepted: 15 November 2018

Rao & Selvamani (2015) highlighted data security related trials and proposed a solution for the same. Advanced encryption schemes can be used for cloud data security and an efficient key management technique must be used for valid data access authorization. Ali, Khan & Vasilakos (2015) presented a survey on recent cloud computing and mobile cloud computing security solutions. The tabulated analysis and comparisons of different security techniques help to analyze and extract the best suited security approach. Soceanu et.al, (2015) put forward a new security system which incorporates an encryption pattern and ABAC. The access control mechanism research is based on XACML, specified by OASIS. SAFAX, a novel authorization context advanced by the Eindhoven University of Technology has been used in the research for patient's data access applicability and feasibility verification.

Choi & Paderes (2015) proposed a biometric application to secure the healthcare records stored on the cloud. This approach provides the logged information about health workers who accessed the health records.

Bokhari, Shallal & Tamandani (2016) reviewed different security issues and architectures to get lower computation cost. As cloud user does not know where his data is being stored actually so it is mandatory for the data owners to know about cloud security level before migration to cloud. Azaria et.al (2016) proposed a distributed record managing structure called MedRec by blockchain technology. This system can manage security and privacy issues like confidentiality, authentication, and accountability for the sensitive medical data. Accessibility, auditability and interoperability have been provided to handle medical records using a comprehensive log. Ibrahim, Mahmood & Singhal (2016) offered a context for secure interchange of EHRs among healthcare service providers and patients. This scheme requires simply three message conversations for authentication and one message conversation for medical information retrieval.

Fernando et.al. (2016) anticipated an effective and access control that is fine grained for EHRs in the cloud. Authors proposed a set of security mechanisms with a fine-grained access management. Zhou et.al. (2016) proposed an identity, privacy and security scheme called unidentified Role-Based Access Control (RBAC) for electronic health records (EHR). They encapsulated EHR data as per its on-demand access policy. Yang, Zheng & Fan (2017) proposed a privacy-preserving, trustworthy, searchable and secure e-healthcare scheme, which supports forward privacy and delegated verifiability. The sensitive PHI data stored on cloud is secured through dynamic searchable symmetric encryption (SSE) scheme. Sanchez-Guerrero et.al. (2017) proposed an enhanced cloud healthcare data privacy scheme based on selective identity information discloser. To make more reliable and powerful role of patients, authors have used adaptive extended Markle tree for user's profile representation.

Verma, Tyagi & Malik (2017) explored the issues pertaining to privacy and security of outsourced data in cloud storage. Authors also reviewed different attribute based encryption techniques with their merits and demerits. Muller, Ludwig & Franczyk (2017) discussed about cloud user data privacy and raised a question about cloud integration with the decentralized information system. Authors have presented a classification assessment from the social networks and found that peer-to-peer approach is mostly favored because they do not need any central authority.

Shahmoradi et.al, (2017) analyzed the electronic health record (EHR) system for its strengths, weaknesses, threats, and opportunities at the Tehran University of Medical Sciences (TUMS) with the participation of 90 members' workforce. The collected data is analyzed by SPSS software. The result shows that the weakness is lack of hardware and infrastructure and strength is being to timely and quick access to information. Els & Cilliers (2017) investigated about data security control of personal electronic health records (PEHRs) being accessed from mobile devices. The Authors have used mobile health privacy context and identified ten privacy ethics for personal healthcare records on mobile devices and recommended to improve the framework through new powerful security controls. Chaudhury et.al. (2017) adopted IoT for the communication and monitoring purpose in Healthcare System. Authors proposed a system which transmits the data through wireless communication after monitoring health parameters. The proposed system can notify the doctors or health service providers via the audio signal in case of any abnormal behavior found in patient's health data. Bandi (2017) proposed a role based encryption, attribute based encryption such as key-policy attribute-based encryption to encrypt patient's health records and to accomplish fine-grained access control of those outsourced health records. Author implemented the key-policy attribute-based encryption system to obtain the fine grained access control policy. Anyone is able to download the patient's data, however only authorized user can decrypt and outlook the patient's health record. Gupta, Verma & Singh (2018) investigated present data encryption systems, like RSA, KP-ABE, CP-ABE, and AES. They compared these algorithms based on computational cost and storage cost. Additional, the authors have offered an improved system to boost the speed of RSA encryption using multi-threading model on latest multi-core CPUs.

Received: 20 October 2018/Accepted: 15 November 2018

III. Proposed Data Classification and Security Framework

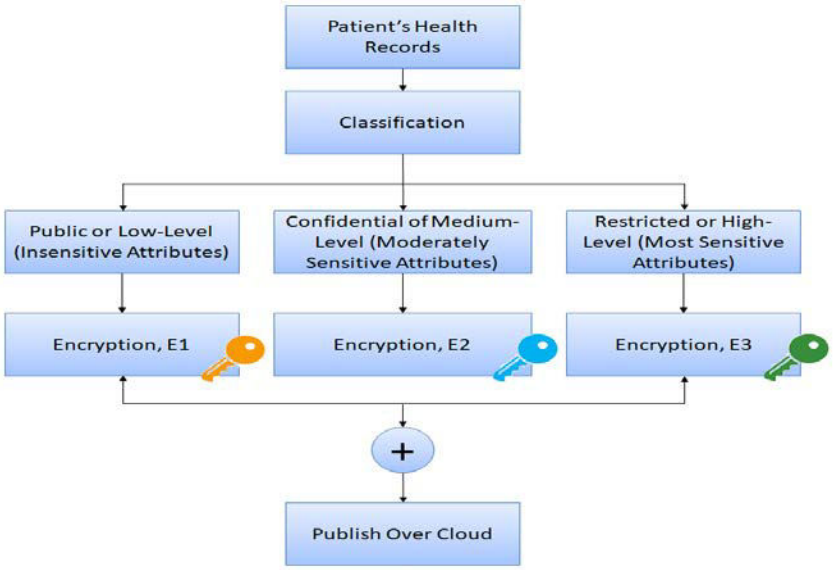

Fig.1: EHR security framework

The objective of the proposed system for maintaining EHRs is to secure them before deploying them for sharing among healthcare providers. The proposed system emphasizes on data classification and encryption (see fig.1).

Table 1: Data Classification Description

Data Classification	Risk level	Example
Restricted or high level	High	Background, Genomic, Psychological health, Obsessions, substance abuse, Sexually-transmitted ailment, Infirmity, Sex life, Behavioral profiles, HIV, UID, Cancer etc.
Confidential or Medium level	Medium	Domestic violence, SSN, Contact No., DoB, Physical health condition, Bank A/C details, blood group, height etc.
Public or low level	Low/None	Caste, nationality, name, X-ray, body temperature, urine test, cardiology test, heart rate, Blood pressure, MRI test etc.

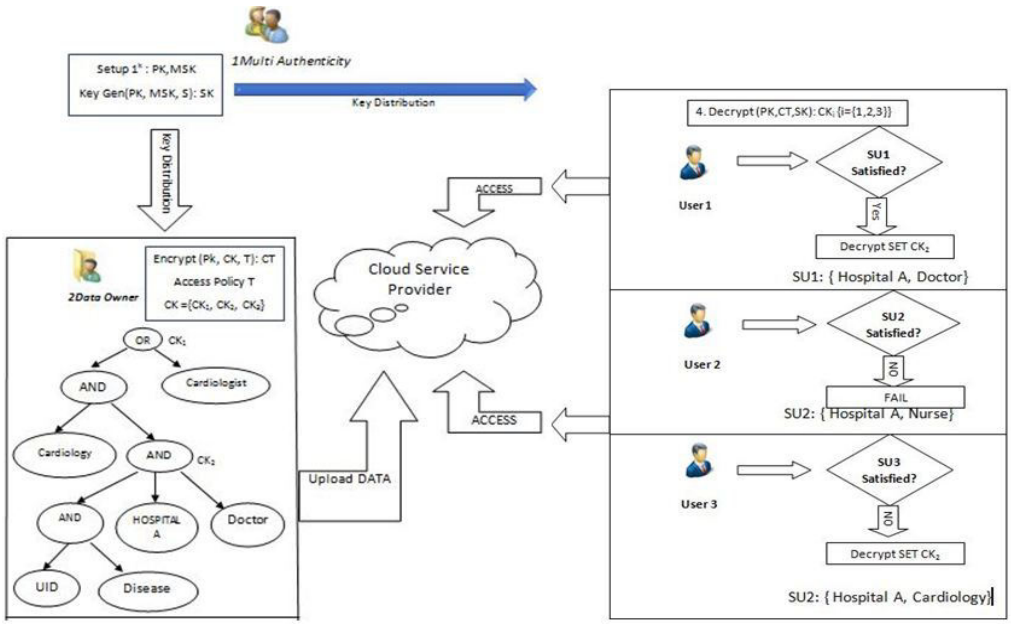

Fig. 2: Layered architecture of generic model for EHR

Received: 20 October 2018/Accepted: 15 November 2018

In Fig. 2, we have explained the working of CP-ABE. The access policy use 'AND' and 'OR' gates with different secret keys.

Patient Data Classification

We can classify the patient data based on critical diseases by using document classification techniques such as KNN, SVM, Naïve-bayes, NN and random forest. Likewise, there are different encryption algorithms with different key generation process, we can play with them. We can choose the encryption algorithm based on sensitivity of the data.

We have done a classification of patient's disease like cancer and diabetes. In the diabetes dataset we consider the fields like pregnancy, blood-sugar, glucose, skin thickness, insulin, BMI, age, diabetes, etc. Following are the descriptions of the algorithms used in our work.

K Nearest Neighbor (KNN)

This algorithm is suited for the problems of prediction like regression and classification. The trend however in industries focuses more on classification. The evaluation of this technique takes into three aspects.

1. Ease to interpret output
2. Calculation time
3. Predictive Power

Implementation of KNN Model

The implementation of KNN model includes.

1. Insert data
2. Value initialization for k
3. Iteration is performed from 1 till the total points of data
   i. Euclidean distance is used as a metric for distance calculation because of its popularity. It evaluates the test data and training data in each row.
   ii. Ascending order sorting on the values of distance is done.
   iii. The array that is sorted is picked for top row k values.
   iv. Then rows are picked that are most frequent.
   v. Predicted class is returned.
   vi. Parameter Selection.
   vii. The preeminent selection of k depends upon the data; generally, the larger the value less is the noise in the process of classification, which uses boundaries to differentiate the two values. Different types of heuristics can be used for selection of good value of k. the nearest neighboring algorithm is used to evaluate at the value k =1 for finding the training sample with closest value.
   viii. To get rid of tied votes one can use classification with appropriate values of k. Bootstrap method can find the value of k by optimal selection.

Supervised algorithms for learning are powerful methods for classification. The distance between the points can be evaluated by Euclidean and Manhattan methods.

i. Euclidean distance:

The Euclidean distance can be evaluated on a line segment by computing the distance between the points connecting them.

The dataset used in our paper has 22 attributes and includes a space of 22 dimensions. If $x = (x_1, x_2 ... x_{22})$ and $y = (y_1, y_2 ... y_{22})$ are two points in Euclidean 22-space, then d(x, y) is calculated by:

$$d(x,y) = \sqrt{\sum_{i=0}^{n} (xi - yi)^2}$$

ii. Manhattan distance:

The axes that are along the right angles are evaluated to go from point of data to another in Manhattan distance calculation. It is analogous to a street structure by calculation of the shortest distance. The d(x, y) is calculated by:

$$d(x,y) = \sum_{i=1}^{n} |xi - yi|$$

Received: 20 October 2018/Accepted: 15 November 2018

Data Encryption Methodologies

One of the methods to classify a patient's health level is done based on its sensitivity. More security is needed for data that gas high sensitivity when compared to the one with lower. Classification of data is done is done on the following measures of information, sensitive, personal, medical, physical health conditions and financial. For any kind of medical record it is important to restrict the privacy of health data to avoid its exposure to sources for which it is not meant and to restrict its inappropriate usage. Based on such parametric requirements, different type's encryption algorithms are available which cater to the sensitivity of the data processed. Algorithms like Rivest-Shamir-Adleman (RSA) Algorithm, Blowfish, IDEA, Advanced Encryption Standard (AES) Algorithm and Ciphertext Policy Attribute Based Encryption (CP-ABE) Algorithm assess the sensitivity level of data and can be used effectively. For example, a usual person does not entail special security but a well-known personality needs a body guard i.e. the intensity of security is proportionate to the cost of asset it safeguards. We have proposed some security mechanisms which are safe and can be used to store medical records in encrypted form after data classification. The requirement is to distinguish the data based on different levels of sensitivity, so that confidentiality of the health report of the patient is maintained. Any adversary would not be capable to outlook a patient's health record as such records are stored on cloud that is not easy to get to by one and all, protection becomes a foremost apprehension. Encryption is possibly the most fool proof method by which the confidentiality of the electronic health documents can be preserved. Separate entities can be created to classify the data which are in turn records and is based on how sensitive the data is. This is a different approach to look at the health records of the patients stored electronically. Further a database is used to store the classified data. We have the idea of classification of the data based on the sensitivity level. If we automatically classify the data then the overhead time of processing the EHRs can be reduced effectively. For example, it is not a good practice to encrypt a 100 GB data block fully using the matching key size and security level as it could only comprise twenty percent of trusted data. In Machine learning, the method of classification is used to separate unclassified and classified data. The existing literature survey shows that manual classification is mostly taken up. We propose an automatic classification for the patients data based on sensitivity level using KNN classification algorithm. KNN is a supervised machine learning technique that is the simplest iterative procedure to classify unclassified datasets into user specified classes. For the details of classification criteria see table 1. Categorization of the patient's data is done into three parts such as Low level, Medium level and High level according to their sensitivity. Encryption on the data that is classified can be done using different types of encryption schemes. The insensitive attributes (Public data) do not require very complex and slow encryption algorithms like AES, RSA or CP-ABE. Deciding on an encryption scheme which is appropriate for each proposed level is also done on frequency of accessing the EHR data. Accessing the low level EHR data is slower than the one at greater frequency than medium level or high level EHR data. The Greater speed of processing with low or no security measures is essential for encryption scheme for low level HER. We have proposed DES and IDEA encryption scheme for the low level EHR data. The IDEA has a weak key problem and DES suffers from Brute force attack but they can still be used for low level EHR data because of low or no requirement of security for this level. Because of encryption speed, IDEA can be stated as a better option at this level. Confusion and diffusion are used by the IDEA algorithm in its encryption process. Different from other block cipher methods, IDEA uses incompatible algebraic operations XOR, module 216 addition, and multiplication modulo 216 + 1. This multiplex operation modulo 216 + 1 replaces the Substitution Box (S-Box). The IDEA algorithm uses multiplication modulo 216 + 1 with the consideration that multiplication with zero always yields zero and has no inversion. The number 65537 (216 + 1) is a prime number. Therefore, modulo multiplication operation (216 + 1) on the IDEA algorithm has an inversion, if forming a multiplication table for numbers ranging from 1 to 65536, each row and column contains only one number once. In IDEA, for multiplication operations, a 16-bit number consisting of zeros is all considered a number 65536, while other numbers remain under the unmarked numbers it represents. More security is needed at the Medium Level EHR in comparison low level EHR data. Hence the algorithms that are more suitable for protection at Medium Level EHR are Blowfish, 3DES, Diffie-Hellman and ELGAMAL. Blowfish is better in terms of speed when compared to ELGAMAL, Diffie-Hellman and 3DESbased on our experimental analysis. Hence Blowfish algorithm is chosen for fastest accessibility and security requirement for the medium level EHR data. It uses a shared key for encryption and decryption. This encryption scheme works well using smaller memory, making it suitable for medium level EHR data security. Blowfish encryption algorithm presents with one limitation that is the size of the file which cannot be greater than 4GB due to its small block size. However such limitation does not change much our proposed architecture. A faster cipher method is Blowfish which works well except for key exchange part. Pre-processing is equivalent for encrypting texts of 4 kbs only hence it is slow. It is a problem in certain applications but a decent approach in others. 4 kilobytes of RAM is the memory requirement for Blowfish implementation. Except for its restriction in embedded systems; like smartcards the above states constraint is not of much concern.

Received: 20 October 2018/Accepted: 15 November 2018

Because of its easy availability and no patents attached to it, Blowfish was one of the first secure blocks thus making it a popular choice in the cryptographic networks. bcrypt uses hashing function with passwords and under various repetitions of work in terms of cost. It works on the key setup which is costly for blowfish and increases the time for evaluation of hash calculation and lessening the attacks by brute force. The High Level EHR data requires strongest security than low level EHR data. We have selected AES, CP-ABE, and RSA to enforce high level restriction on EHR data. AES-256 encryption scheme uses key lengths of 128, 192 or 256 bits. AES encryption is never compromised because of its security strength. If someone wants to break its security, then 2^{256} key combinations are impossible to calculate. CP-ABE can also be used for high level security that also ensures the access policy efficiency. RSA algorithm also delivers strong security but suffers from the low encryption and decryption speed. RSA can be used if data size is small enough. In few cases, RSA is not advisable because of its undesirable slow speed only. So as the conclusion, AES or CP-ABE encryption scheme is the best for this level data. We preferred CP-ABE more than AES because of its useful access policies and other security strengths.

(1) Setup: The attribute authority uses the master key (MK) for generating the secret keys (SK) for the users in this phase.
Setup :{ λ} → {MK, PK}
(2) Encrypt: This phase generates a ciphertext (CT) using a plaintext (M) and a public key (PK).
(3) Enc :{PK, MK, A}→ CT
This phase generates a secret key (SK) using a set of attributes w, which are relates to user and master key (MK).
KeyGen: {MK, w} → SK
(4) Decrypt: This phase decrypts a ciphertext with the help of secret key (SK) for getting the actual message (M) after satisfying the access policy associated with access tree.
Dec: {SK, CT} → M

Table 2: Encryption algorithm analysis and comparison for different level security of EHR data.

Sr. No.	Algorithm	EHR Risk Level	Key Size (bit)	Speed	Security Strength/Weakness Remark
1	DES	Low	56	Fast	Vulnerable to differential and linear cryptanalysis
2	3DES	Medium	192	Slow	Vulnerable to differential and brute force attack.
3	BLOWFISH	Medium	64	Very Fast	Vulnerable to dictionary attack
4	IDEA	Low	128	Fast	Vulnerable to differential timing attack, Key-schedule attack
5	AES	High	128	Fast	Robust against differential, reduced differential, linear, interpolation and square attacks
6	DIFFIE-HELLMAN	Medium	128	Moderate	Vulnerable to man-in-the-middle attack
7	ELGAMAL	Medium	256	Slow	Vulnerable to chosen ciphertext attack
8	RSA	High	2048	Slow	Attacker can launch chosen-ciphertext attack
9	CP-ABE	High	23848	Fast	Most secure

IV. Experimental Analysis

The algorithms are executed using Java 8 with Intel core i5 CPU of 2.40 GHz with 4 GB of RAM. We used diverse magnitude of text documents in our execution such as 32 KB, 64 KB, 128 KB, 256 KB and 512 KB.

Patient Type Classification

Here, we are presenting results of patient type based on the given data using different classification algorithms. In this work, we have implemented three classification approaches and the corresponding results are presented in Table XX, where KNN provides the best outcome for the classification based on patient's disease.

Table 3: Outcome percentage of different classification algorithms

S. No	Algorithms Used	Outcome(in percentage)
1	k Nearest Neighbour(KNN)	78
2	Support Vector Machine(SVM)	76.8
3	Neural Network(NNET)	75.5
4	Random Forest(RF)	75.5
5	Naïve Bayes(NB)	50

Received: 20 October 2018/Accepted: 15 November 2018

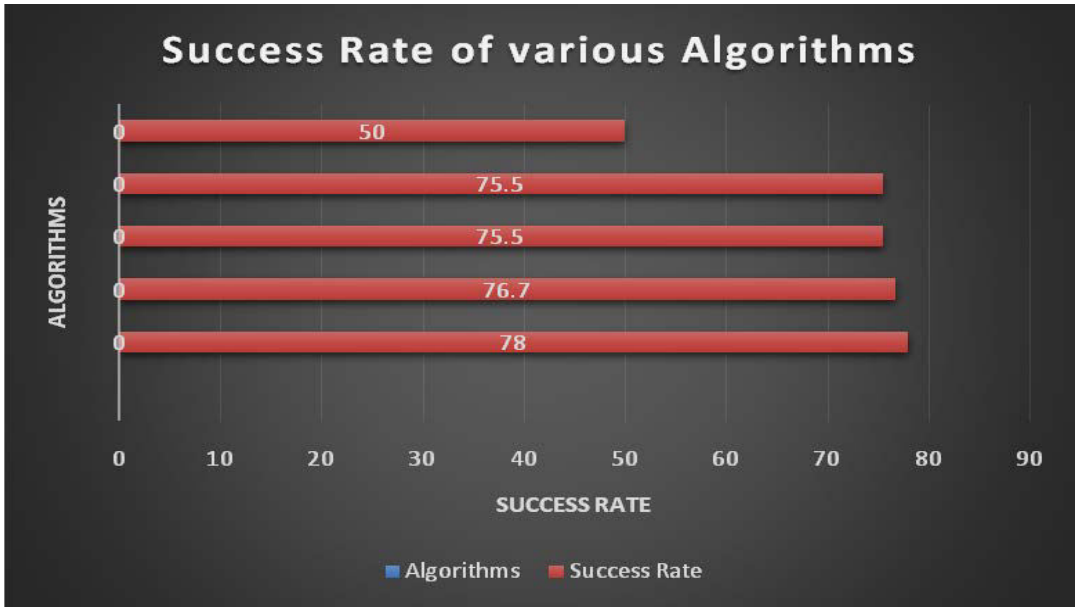

Fig 3: Comparison of Success Rate of various Algorithms

Data Encryption/Decryption Performance

We have taken the different parameters like encryption/decryption time and key generation time for calculating the performance of various encryption and decryption methods like DES, 3DES, Blowfish, IDEA and AES as symmetric methods and RSA, Diffee-Hellman, CP-ABE and Elagamal for asymmetric methods. The encryption, decryption and key generation times are shown in milliseconds for all file sizes in all the algorithms.

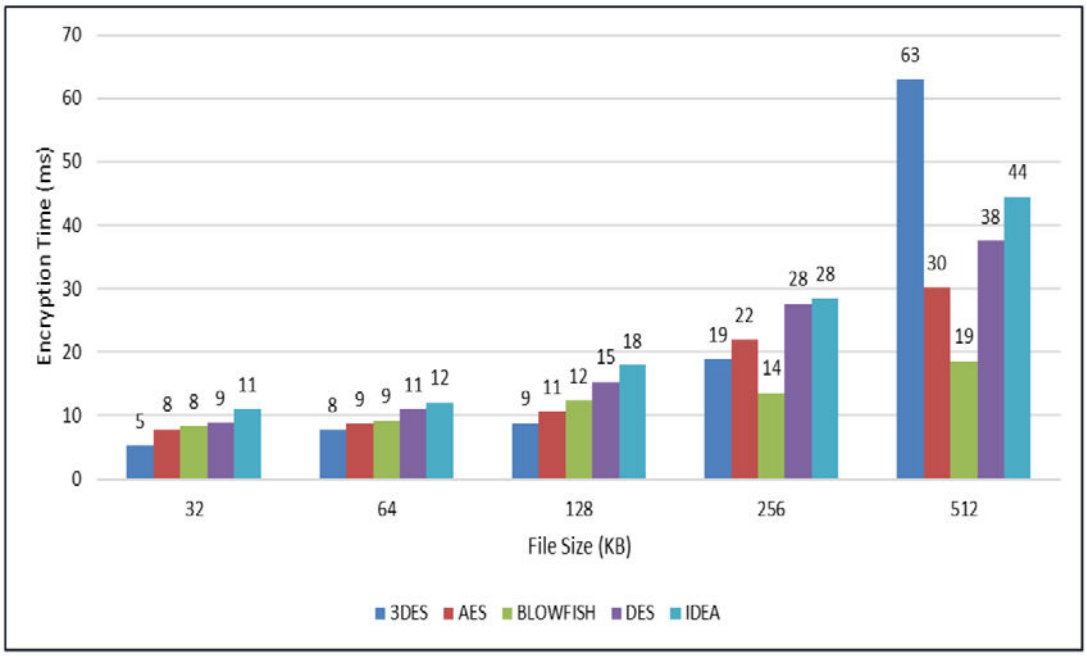

Figure 4: Encryption time of symmetric encryption algorithms.

Figure 4 demonstrates the encryption time comparison among symmetric encryption algorithms. One can observe that blowfish has a good impact over throughput in encryption time when file size increases. 64-bit key size has been used for all files in blowfish encryption.

Received: 20 October 2018/Accepted: 15 November 2018

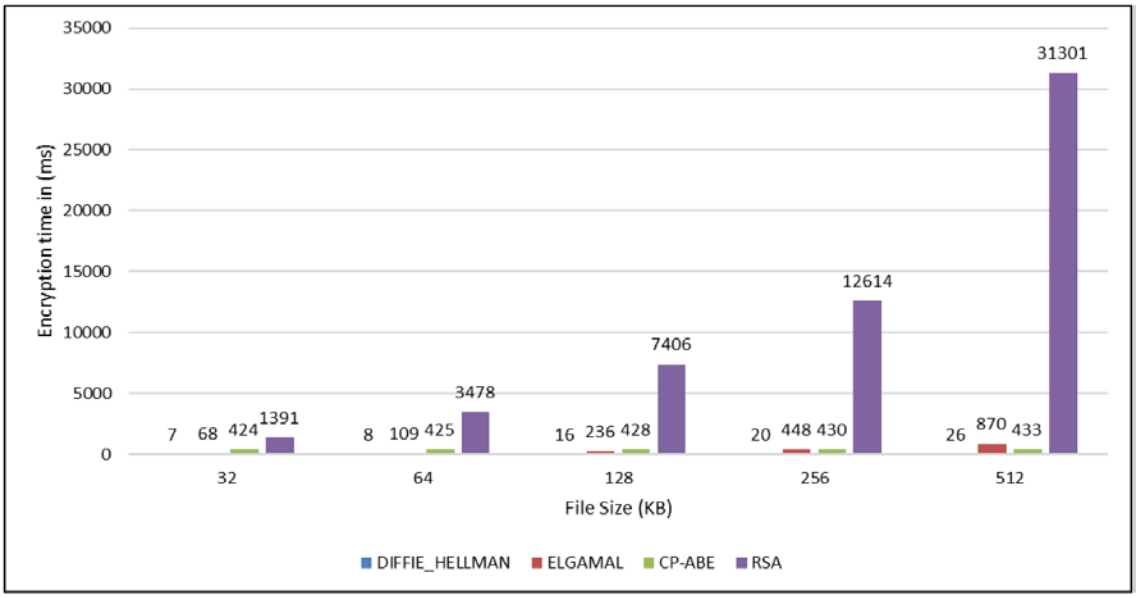

Figure 5: Encryption time of asymmetric encryption algorithms.

Other symmetric encryption algorithms have multiplying rate for the encryption time. AES stands on the second place after blowfish. 3DES encryption time data for different file sizes shows that this algorithm's throughput performance is not efficient for larger file size. Figure 5 shows the encryption time comparison among asymmetric encryption algorithms. One can observe the significant time difference in encryption time between symmetric and asymmetric methods. Asymmetric methods use diverse keys for encryption and decryption. Asymmetric algorithms require much more encryption time than symmetric algorithms. As both figures suggest that asymmetric algorithms are too slow than symmetric algorithms. We can observe from the Figure 3 that Diffie-Hellman has the lowest computation time in data encryption. CP-ABE stands on the second place in the comparison of computation time among all four asymmetric algorithms. RSA algorithms deliver the stronger data security but struggles from very high computation cost than other algorithms.

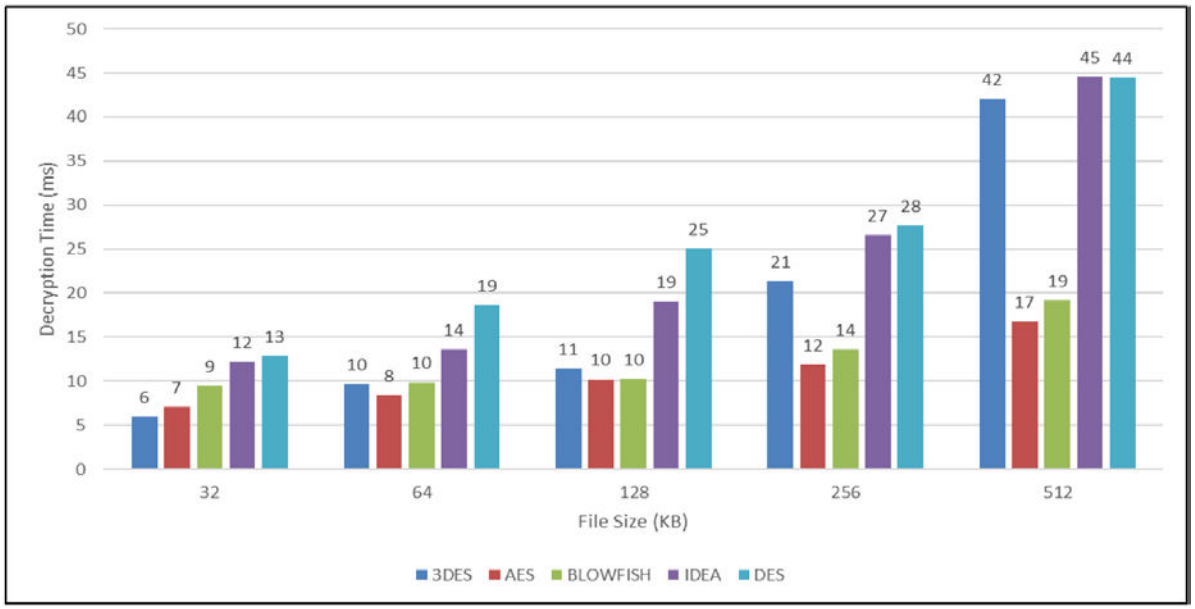

Figure 6: Decryption time of symmetric encryption algorithms.

Figure 6 shows that AES consumes the lowest computation time among all five selected symmetric algorithms in decryption phase. A blowfish algorithm is on second place as it consumes more computation time than AES. We can observe from Figure 3 and Figure 4 that Blowfish or AES can be selected if better throughput is required in

Received: 20 October 2018/Accepted: 15 November 2018

outsourced data security. Although a successful brute force attack has never been performed on both encryption algorithms, Blowfish is not so popular than AES algorithm. Blowfish uses key sizes from 32 bits to 448 bits whereas AES-256 allows 128-bits, 192-bits, and 256-bits keys for encryption and decryption process. Blowfish allows selection of vast range of key sizes but still AES is better choice for someone who is going to select symmetric algorithm for data security. Figure 7 show that Diffie-Hellman has the best decryption rate than other asymmetric algorithms. CP-ABE still settled on second place as was in encryption time comparison. RSA takes huge amount of decryption time which is greater than encryption time for the same file size because of some extra calculation. If performance is not a big deal, CP-ABE could be better approach for security reasons. Figure 8 displays the key generation time in symmetric and asymmetric algorithms. 3DES has the largest key generation time in the group of selected symmetric algorithms. CP-ABE consumes highest key generation computation time in asymmetric algorithms. Although IDEA algorithm has the lowest computation time at key generation phase, still AES is better selection on behalf of its security strength. Diffie-Hellman has the lowest key generation computation time for the 128-bit key size in the group of asymmetric algorithms. We have used 2048-bit RSA, 128-bit Diffie-Hellman and 256-bit ElGAMAL key sizes. The new key generation in Diffie-Hellman algorithm is very fast. Although RSA and Diffie-Hellman work on identical mathematics, as RSA uses integer factorization and Diffie-Hellman uses discrete logarithm. Both algorithms serve for different purpose as RSA is mostly used for digital signature generation and encryption whereas Diffie-Hellman is mainly used for key agreement. RSA is out of fashion today and in case of SSL security, Diffie-Hellman is better selection to achieve forward secrecy. Strength of Diffie-Hellman algorithm is that it authenticates both encryptor and decryptor whereas RSA only authenticates receiver.

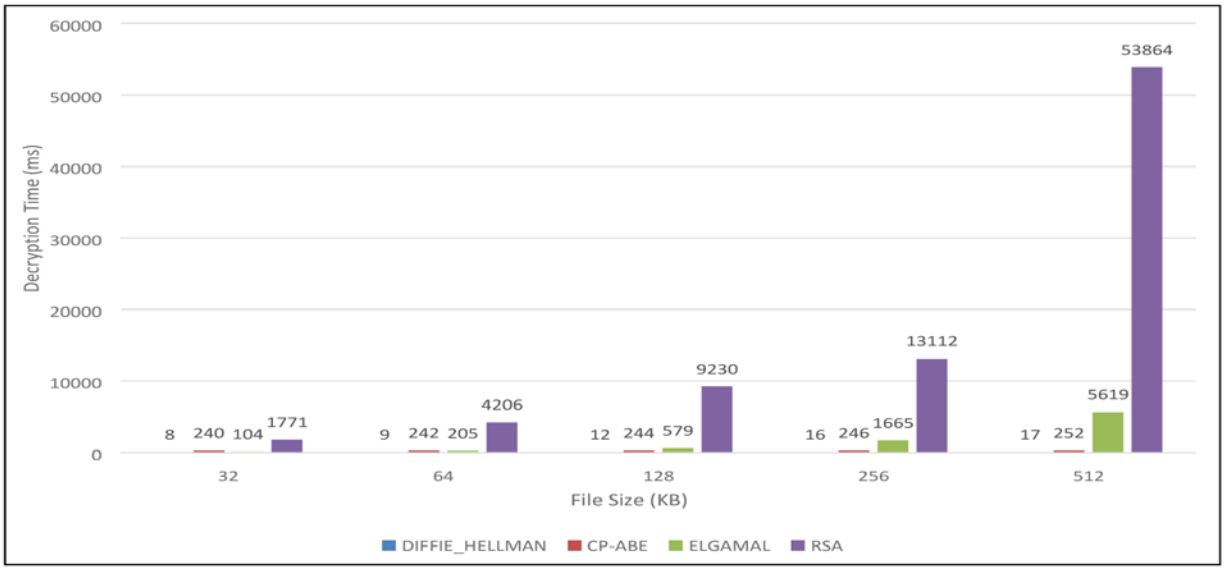

Figure 7: Decryption time of asymmetric encryption algorithms.

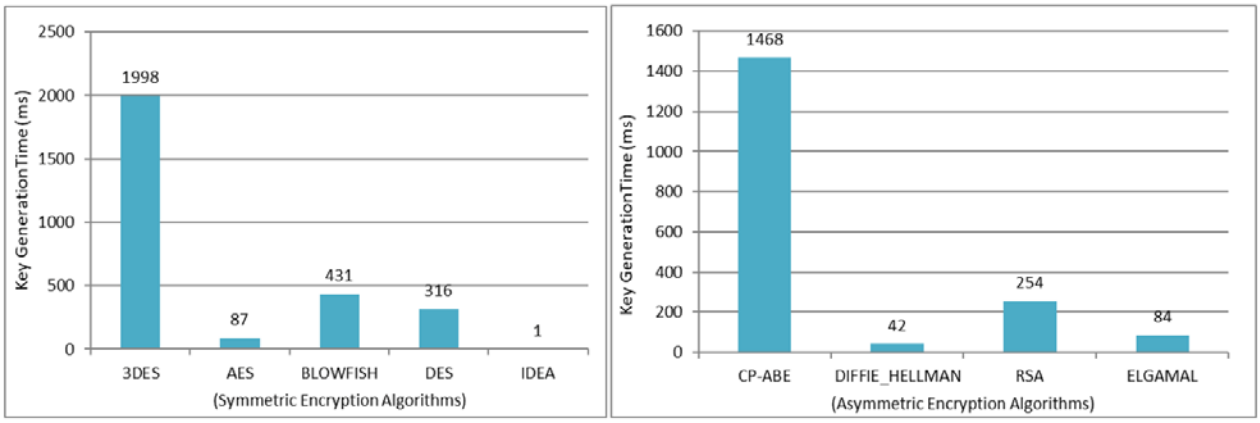

Figure 8: Key generation time of symmetric and asymmetric encryption algorithms.

Received: 20 October 2018/Accepted: 15 November 2018

V. Conclusion

EHRs have transformed the present healthcare scheme and enhanced the patient-doctor adroitness. Vulnerability of health data records arises due to lack of appropriate security actions. The proposed scheme aims to provide a high level of patient's health data security using classification on the basis of their sensitivity levels. Ciphertext Policy Attribute based encryption (CP-ABE) is used to accomplish encryption. We have compared symmetric encryption algorithms such as DES, 3DES, Blowfish, IDEA, AES and asymmetric encryption algorithms such as RSA, DIFFIE_HELLMAN, ELGAMAL and CP-ABE for achieving confidentiality of health data stored in cloud.

References

[1] Ali, M., Khan, S. U. and Vasilakos, A. V. Security in cloud computing: Opportunities and challenges. *Information Sciences* **305** (2015) 357-383.

[2] Amato, F., Casola, V., Mazzeo, A. and Romano, S. A semantic based methodology to classify and protect sensitive data in medical records. *Sixth International Conference on Information Assurance and Security (IAS),* 2010, 240-246.

[3] Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. Medrec: Using blockchain for medical data access and permission management. *International Conference on Open and Big Data (OBD),* 2016, 25-30.

[4] Bandi, R. S. J. B. P. Securing E-healthcare records on Cloud Using Relevant data classification and Encryption. *International Journal of Engineering and Computer Science* **6** (2) (2017).

[5] Bokhari, M. U., Shallal, Q. M. and Tamandani, Y. K. Security and privacy issues in cloud computing. *3rd International Conference on Computing for Sustainable Global Development (INDIACom),* 2016, 896-900.

[6] Bollineni, P. K. and Neupane, K. Implications for adopting cloud computing in e-Health, 2011.

[7] Chaudhury, S., Paul, D., Mukherjee, R. and Haldar, S. Internet of Thing based healthcare monitoring system. *8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON),* 2017, 346-349.

[8] Choi, M. and Paderes, R. E. O. Biometric Application for Healthcare Records Using Cloud Technology. *8th International Conference on Bio-Science and Bio-Technology (BSBT),* 2015, 27-30.

[9] Verma, D.K, Tyagi, R.K. and Malik, K. Privacy and security issues of outsourced data in EHR in *International Conference on Technology & Trust (ICTT'17),* 2017, 98-103.

[10] Els, F. and Cilliers, L. Improving the information security of personal electronic health records to protect a patient's health information. *Conference on Information Communication Technology and Society (ICTAS),* 2017, 1-6.

[11] Fakhar, F. and Shibli, M. A. Comparative analysis on security mechanisms in cloud. *15th International Conference on Advanced Communication Technology (ICACT),* 2013, 45-50.

[12] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O. and Toval, A. Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics* **46** (3) (2013) 541-562.

[13] Fernando, R., Ranchal, R., An, B., Othman, L. B. and Bhargava, B.. Consumer Oriented Privacy Preserving Access Control for Electronic Health Records in the Cloud. *IEEE 9th International Conference on Cloud Computing (CLOUD),* 2016, 608-615.

[14] Ghazvini, A. and Shukur, Z. Security challenges and success factors of electronic healthcare system. *Procedia Technology* **11** (2013) 212-219.

[15] Gupta, P., Verma, D. K. and Singh, A. K. Improving RSA Algorithm Using Multi-Threading Model for Outsourced Data Security in Cloud Storage. *8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2018, 14-15.

[16] Ibrahim, A., Mahmood, B. and Singhal, M. A Secure Framework for Medical Information Exchange (MI-X) between Healthcare Providers. *IEEE International Conference on Healthcare Informatics (ICHI),* 2016. 234-243.

[17] Martínez, S., Sánchez, D. and Valls, A. A semantic framework to protect the privacy of electronic health records with non-numerical attributes. *Journal of Biomedical Informatics* **46** (2) (2013) 294-303.

[18] Mohamed, E. M., Abdelkader, H. S. and El-Etriby, S. Enhanced data security model for cloud computing. *8th International Conference on Informatics and Systems (INFOS),* 2012.

[19] Muller, A., Ludwig, A. and Franczyk, B. Data security in decentralized cloud systems–system comparison, requirements analysis and organizational levels. *Journal of Cloud Computing* **6** (1) (2017).

[20] Rao, R. V. and Selvamani, K. Data security challenges and its solutions in cloud computing. *Procedia Computer Science* **48** (2015) 204-209.

Received: 20 October 2018/Accepted: 15 November 2018

[21] Sanchez-Guerrero, R., Mendoza, F. A., Díaz-Sánchez, D., Cabarcos, P. A. and López, A. M. Collaborative eHealth Meets Security: Privacy-Enhancing Patient Profile Management. *IEEE journal of biomedical and health informatics* **21** (6) (2017) 1741-1749.

[22] Shahmoradi, L., Darrudi, A., Arji, G. and Nejad, A. F. Electronic Health Record Implementation: A SWOT Analysis. *Acta MedicaIranica* **55** (10) (2017).

[23] Shaikh, R. and Sasikumar, M. Data classification for achieving security in cloud computing. *Procedia computer science* **45** (2015) 493-498.

[24] Soceanu, A., Vasylenko, M., Egner, A. and Muntean, T. Managing the privacy and security of ehealth data. *20th International Conference on Control Systems and Computer Science (CSCS),* 2015, 439-446.

[25] Yang, L., Zheng, Q. and Fan, X. RSPP: A Reliable, Searchable and Privacy-Preserving e-Healthcare System for Cloud-Assisted Body Area Networks, 2017.

[26] Zhou, X., Liu, J., Liu, W. and Wu, Q. Anonymous Role-Based Access Control on E-Health Records. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, 559-570.

[27] Ozair, F. F., Jamshed, N., Sharma, A. and Aggarwal, P. Ethical issues in electronic health records: a general overview. *Perspectives in clinical research* **6** (2) (2015).

Received: 20 October 2018/Accepted: 15 November 2018

RESEARCH ARTICLE OPEN ACCESS

A Survey on Data Integrity Auditing Schemes in Cloud Computing

Purnima [1], Deepak Kumar Verma [2]
Student of MTech. [1]
Computer Science Department [2]
IEC College of Engineering and Technology, Greater Noida
Uttar Pradesh, India.

ABSTRACT
Cloud computing is an inclusive new approach on how computing services are produced and utilized. Cloud computing is an accomplishment of various types of services which has attracted many users in today's scenario. The most attractive service of cloud computing is Data outsourcing, due to this the data owners can host any size of data on the cloud server and users can access the data from cloud server when required. The new prototype of data outsourcing also faces the new security challenges. However, users may not fully trust the cloud service providers (CSPs) because sometimes they might be dishonest. It is difficult to determine whether the CSPs meet the customer's expectations for data security. Therefore, to successfully maintain the integrity of cloud data, many auditing schemes have been proposed. Some existing integrity methods can only serve for statically archived data and some auditing techniques can be used for the dynamically updated data. In this paper, we have analyzed various existing data integrity auditing schemes along with their consequences.

Keywords :— Third Party Auditor (TPA), Cloud Service Providers (CSPs), Data Outsourcing, Proof of Retrievability (POR), Provable data Possession (PDP).

I. INTRODUCTION

Cloud computing is widely embraced by many organization and individuals because of its various dazzle advantages like huge size data storage, cumbersome computation, low price service and flexible way to access the data [1], [14]. The basic concept behind cloud computing is virtualization. In cloud computing, virtualization means to create a virtual variation of a device or resource, such as a server, storage device, network or operating system where the structure divides the resource into required number of execution environments [32]. Cloud computing is a predominant service of cloud storage, which allows data owner to store their data from their local computing system to cloud. Many users store their data on cloud storage. However new protocol of data hosting service also introduces security issue [6]. Data owner would be worry that data could be lost in the cloud. Therefore, the biggest concern is how to determine whether a cloud storage system and service provider meet the customer expectations for data security [20]. Therefore, it is crucial and significant to amplify efficient auditing scheme to strengthen data owners′ faith in cloud storage. Various types of auditing models have been proposed, they can be categorized into two types Private auditing model and Public Auditing Model. Traditionally in Private auditing model data owner can verify the integrity of outsourced data based on the two-party storage auditing protocol. In this technique data owner should have expertise. It increases the overhead of data owner and sometimes it also happens both data owner and CSP cannot convince each other for the result.

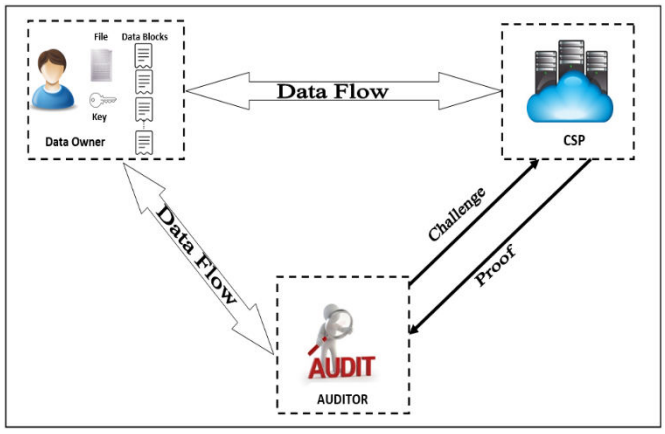

Figure 1. Cloud Auditing Model.

As public auditing is the advisable model for outsourced data verification, it additionally involves the third party to check the integrity [3], [5], [14] which can provide equitable auditing result for both data owner and CSP. Data owner send metadata to TPA instead of original data. Basically, auditing model has two phases set up phase and verification

phase. Data owner has to perform some operations prior to send data to TPA [5].

II. RELATED WORK

In the contemporary year, cloud storage auditing has attracted attention to strengthen data owners' trust and confidence in cloud storage. To verify the integrity of outsourced data many protocols have been proposed with distinct techniques [4], [7], [8], [12], [15], [16], [18], [20], [21], [22], [26]. The first auditing related work was introduced in 2007 by Juels et al. is POR (Proof of Retrievability) [4] scheme, which can check the correctness of data with the use of error correcting code. It is typically a private auditing model because there is no existence of any other third party. In the same year, Atenies et al. [16] has introduced first public Auditing Model, PDP using Homomorphic tag based on RSA. It does not support privacy preserving of data. Beside data integrity auditing there are many other significant concerns such as privacy-preserving, batch auditing, and dynamic auditing. In 2008, Atenies et al. [20] has further proposed the scheme which supports dynamic auditing but does not preserve privacy.

In 2009 Erway et al. [12] proposed dynamic PDP scheme that does not require privacy preserving. In 2010, First privacy preserving PDP was introduced by Wang et al. [6], they presented a public auditing scheme which ensures the privacy preserving for outsourced data using integrating Homomorphic authenticator with the random masking technique. In 2012 further, a new public auditing scheme Cooperative PDP (CPDP) technique proposed by Zhu et al [7], which was based on hash index hierarchy and Homomorphic verifiable scheme. It Supports public auditing, Privacy preserving and Batch auditing in the multi cloud but it has no provision for multi-user auditing. Dynamic Auditing Protocol (DAP)in 2013, Yang et al. [15] proposed further enhanced auditing schemes which supported dynamic auditing using the Index table scheme. In 2015, Identity-Based Distributed Provable Data Possession (ID-DPDP) scheme was proposed by Wang, Huaqun [26] which used bilinear pairing in random access model.

Dynamic Hash Table-Public Audit (DHT-PA) introduced by Hui Tian et al. [14] in 2016 proposed Dynamic hash table which supported public dynamic auditing. Dynamic hash table supports public dynamic auditing and employed Homomorphic authenticator with random masking to preserve the privacy of outsourced data. They used aggregate BLS signature to arrange batch auditing.

III. LITERATURE SURVEY

Data Integration Scheme	Technique	Proposed By	Year	Strength	Weakness
POR (Proof of Retrievability) [4]	Using error correcting code	Juels et al.	2007	• Private Auditing using error code • Data recovery is possible	• Increase overhead on Data Owner. • Cannot be used in the original form, preprocessing is required for encoding.
PDP (provable data possession) [16]	Use Homomorphic tag based on RSA	Atenies et al.	2007	• Support public auditing	• Not Privacy preserving • No Batch auditing • Communication overhead • Data recovery is not supported
Partially Dynamic – PDP [20]	Symmetric Key Cryptography	Atenies et al.	2008	• Supports Dynamic Auditing	• No Privacy preserving • Bounded no of

					Audits.
CPR (Compact Proof of Retrievability) [21]	HLA Built from secure BLS-Signature	H. Shacham, B. Waters	2008	• Improved POR scheme	• No Privacy preserving
DPDP (Dynamic PDP) [12]	Using ranked based authenticated skip list	Erway et al.	2009	• Dynamic data auditing • No demand of privacy-preserving	• No public auditing • Not support Batch auditing • Not Privacy preserving
PDP First privacy preserving [7]	Integrating the Homomorphic authenticator with random masking	Wang et al.	2010	• Supports public auditing • Privacy preserving	• Does not support data dynamics
Fully Dynamic PDP [22]	Combined BLS based HLA with MHT	Wang et al.	2011	• Supports Dynamic Auditing	• Not Privacy preserving
CPDP (corporative provable possession) [8]	Hash Index Hierarchy	Zhu et al.	2012	• Support public auditing • Privacy preserving • Batch auditing in multi cloud	• It does not support dynamic audit • Does not support auditing for multiuser
DAP [15]	Index table	Kan Yang et al.	2013	• Support public auditing • Privacy preserving • Support dynamic auditing • Batch auditing in multi-cloud	• High Computation cost
DPDP-MHT [19]	Based on Merkle hash tree	Wang et al.	2013	• Support public auditing • Privacy preserving • Support dynamic auditing • Batch auditing in multi-cloud	• Heavy computation cost of the TPA • Large communication overhead
IHT-PA (Index hash table-public audit) [18]	Index Hash table	Zhu et al.	2013	• Support public auditing • Privacy preserving • Support dynamic auditing	• Batch auditing is not mentioned

MUR-DPA [2]	Used Authenticated Data Structure (ADS) based on the Merkle Hash Tree (MHT)	Liu, Chang, et al.	2014	• Provides facility to verify cloud data storage with multiple replicas.	• Works only with constant-sized integrity proofs
ID-DPDP [26]	Distributed Provable Data Possession in Multi-cloud storage.	Wang, Huaqun	2015	• Bilinear pairings in random oracle model Flexible and improves the efficiency.	• Verification delay occurs
DHT-PA (Dynamic hash table-public audit) [14]	Dynamic Hash table	Hui Tian et al.	2016	• Support public auditing • Privacy preserving • Support dynamic auditing • Batch auditing in multi cloud	• Communication cost is greater than DAP and IHT-PA

Table 1: Comparison of existing data integrity auditing schemes [5]

IV. CONCLUSION

In cloud computing, a new paradigm of data outsourcing increases new security challenges. This new paradigm requires a Third-Party Auditor to check the data integrity in cloud storage. In this paper, we have compared different types of auditing schemes on the basis of Privacy preservation, dynamic auditing and batch auditing along with their strength and weakness. From all these papers, it is concluded that there is need to design some optimizing techniques that can be applied to speed up the set phase at data owner side [2], [20], [32]. In our previous paper, we have proposed a multithreading model on multi-core CPU system to generate the signature for each block [5], it is one-time operation and occurs in setup phase at data owner side.

V. FUTURE WORK

In future, we will focus on enhanced & sophisticated data setup process to reduce the computation and communication overhead at data owner side. To generate authenticator, we use multithreading framework on latest multi-core system to speed up the setup phase. We will use the multithreading model in each step of data setup phase.

REFERENCES

[1] P. Melland, T. Grance, "The NIST Definition of Cloud Computing, technical report", Nat'l Inst. of Standards and Technology, 2009.

[2] Nandini J., Sugapriya N. P., M. S. Vinmathi, "Secure Multi-Owner Data Storage with Enhanced TPA Auditing Scheme in Cloud Computing", International Journal of Advances in Computer Science and Cloud Computing, ISSN: 2321-4058, Vol. 2, Issue: 1, MAY 2014.

[3] C. Wang, S. M. Chow, Q. Wang, K. Ren and W. Lou, ″Privacy-Preserving Public Auditing for Secure Cloud Storage, ″ vol. 62, IEEE Trans. on Computers, no. 2, pp. 362-375, 2013.

[4] A. Juels and B.S. Kaliski Jr., "PoRs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007.

[5] Deepak Kumar Verma, Purnima and Rajesh Kumar Tyagi, "Optimizing the User Side Set-up Phase for Privacy Preserving Public Auditing in Cloud Storage", (manuscript submitted for publication), 2017.

[6] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", vol. 24, IEEE Trans. on Parallel and

Distributed Systems, no. 9, pp.1717-1726, ISSN: 2278 – 1323, 2013.

[7] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", Proc. IEEE INFOCOM, pp. 1-9, 2010.

[8] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", vol. 23, IEEE Trans. Parallel and Distributed Systems, no. 12, pp. 2231-2244, 2012.

[9] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell, ″Cloud Security Auditing: Challenges and Emerging Approaches″, IEEE Security & Privacy, vol. 12, no. 6, pp. 68-74, 2014.

[10] M. S. Giri, B. Gaur, D. Tomar, "A Survey on Data Integrity Techniques in Cloud Computing", Vol. 122, No. 2, International Journal of Computer Applications (0975 – 8887), July 2015.

[15] CH. Mutyalanna, P. Srinivasulu, M. Kiran, "Dynamic Audit Service Outsourcing for Data Integrity in Clouds", Vol. 2 Issue 8, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), AUG 2013.

[16] G. Ateniese, R. B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, ''Provable Data Possession at Untrusted Stores,'' Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), pp. 598-609, 2007.

[17] Mr. Pragnash G. Patel and Sanjay M. Shah, "Survey on data security in cloud computing", Vol 1, Issue 9, International Journal of Engg Research and Tech (IJERT), ISSN: 2278-0181, NOV 2012.

[18] Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu and S. S.Yau, "Dynamic Audit Services for Outsourced Storage in Clouds", Vol. 6, no. 2, IEEE Trans. on Services Computing, pp. 227–238, 2013.

[19] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, ''Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing'', Vol. 22, no. 5, IEEE Trans. on Parallel and Distributed Systems, pp. 847-859, 2011.

[20] A P Shirahatti, P S Khanagoudar, "Preserving Integrity of Data and Public Auditing for Data Storage Security in Cloud Computing", IMACST, Vol. 3, Number 3, JUN 2012.

[11] K. Shinde, V. V. Jog, "A Survey on Integrity Checking for Outsourced Data in Cloud using TPA", International Journal of Computer Applications (0975 – 8887), International Conference on Internet of Things, Next Generation Networks and Cloud Computing, 2016.

[12] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession", proc. ACM Conf. Computer and Comm. Security (CCS'09), pp.213-222, 2009.

[13] Sumalatha M.R., Hemalathaa S., Monika R., Ahila C., "Towards Secure Audit Services for Outsourced Data in Cloud", International Conference on Recent Trends in Information Technology IEEE, 2014.

[14] H. Tian, Y. Chen, C. Chang, "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", Vol. PP, Issue: 99, IEEE Transactions on Service Computing, Manuscript ID, DEC 2016.

. [21] H. Shacham and B. Waters, "Compact Proofs of Retrievability", vol. 5350, Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), pp. 90-107, DEC 2008.

[22] Syed Rizvi, Katie and Abdul, "Cloud Data Integrity Using a Designated Public Verifier," in 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), International Symposium on Cyberspace Safety and Security (CSS) and International Conference on Embedded Software and System (ICESS).

[23] S Lins, S Schneider, and A Sunyaev, "Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing", Vol. PP, Issue: 99 IEEE Transactions on Cloud Computing, TCC-2015-10-0378, JAN 2016.

[24] A Kushanpalli, V. S. Kumar, C. R. Yadav, "A Simulation Study of Outsourcing of Audit Service for Data Integrity in Cloud Computing", Vol. 3, Issue 11, ISSN (Print): 2319-5940, International Journal of Advanced Research in Computer and Communication Engineering, NOV 2014.

[25] D. N. Rewadkar, S. Y. Ghatage, "Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit", International Conference on Control, Instrumentation,

Communication and Computational Technologies (ICCICCT), JUL 2014.

[26] Wang, Huaqun. "Identity-Based Distributed Provable Data Possession in Multicloud Storage", Services Computing, IEEE Transactions on 8.2 (2015): 328-340.

[27] S. Pearson, "Toward Accountability in the Cloud", Vol. 15, no. 4, IEEE Internet Computing, pp. 64–69, 2011.

[28] Cloud Security Alliance,"Top Threats to Cloud Computing", http://www.cloudsecurityalliance.org, 2010.

[29] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services", Vol. 24, no. 4, IEEE Network Magazine, pp. 19-24, July/Aug. 2010.

[30] S. N. Poornima, R. S. Ponmagal, "Secure Preserving Public Auditing for Regenerating Code Based On Cloud Storage", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353, Vol. 21, Issue: 4, APR 2016.

.[31] K. Chen, J. M. Chang, T. Hou, "Multithreading in Java: Performance and Scalability on Multicore Systems", Vol. 60, IEEE Transactions on Computers, NO. 11, NOV 2011.

[32] N. Saravana Kumar, G.V. Rajya Lakshmi, B Balamurugan," Enhanced Attribute Based Encryption for Cloud Computing", Vol. 46, pp 689-696, 2015.

Improving RSA algorithm using multi-threading model for outsourced data security in cloud storage

Purnima Gupta[1], Deepak Kumar Verma[2] and Aswani Kumar Singh[3]
[1] *M.Tech. Scholar, IEC College of Engg. & Tech., Greater Noida, Uttar Pradesh, India.*
[2]*Assistant Professor, CSE Department, IEC College Engg. & Tech., Greater Noida, Uttar Pradesh, India.*
[3]*Software Engineer, Soft-Tech Development Solution, Mughalsarai, Uttar Pradesh, India.*
[1]purnimaa018@gmail.com,
[2]deepak.verma1980@gmail.com,
[3]aswanikumar124@gmail.com

Abstract— **Cloud Computing is a promising technology used by scientific and enterprise communities to access shared resources from anywhere through the internet. Users may also store their sensitive and confidential information on the cloud that requires an eminent encryption scheme and a fine-grained access policy to ensure privacy and security. Disparate obtainable symmetric, asymmetric and Attribute-Based Encryption has appreciable encryption schemes to keep secure the confidential data. In this paper, the authors have analyzed existing data encryption schemes, like RSA, KP-ABE, CP-ABE, and AES. The comparisons among them on the basis of computational cost and storage cost have been shown. Further, the authors have proposed an improving scheme to enhance the speed of RSA encryption using multi-threading concept on latest multi-core CPUs.**

Keywords — Attribute Based Encryption; MA-ABE; RSA; AES; DES; CP-ABE.

1. INTRODUCTION

The popularity of cloud computing services is increasing day by day due to its on-demand sharing of online resources. One of the best public cloud service providers is Amazon web services. It is the first among the top 10 most relevant technologies being adopted today by different organizations [21]. One of the main obstacles for selecting cloud is security; security is the main reason behind the lesser number of real-time and business-oriented cloud applications. Encryption is the foremost tools used to secure the outsourced data in cloud storage.

Various cryptographic methods and other security and privacy methods are adopted to secure outsourced data [18] on cloud. Attribute-Based Encryption (ABE) has become the most popular now a day [3], [13]. ABE is a flexible and one-to-many encryption instead of one-to-one so it has many advantages over the Public Key Cryptography. Besides fine-grained access policy, there is a growing need to secure outsourced data. Existing ABE schemes are unable to fulfil the requirement of efficiency, flexibility and scalability of enterprises.

There are three service models of cloud computing as follows: (i) Software as a Service (SaaS) provide licensing and distribution of software services through a network on demand. (ii) Platform as a Service (PaaS) facilitates with infrastructures for the developers to develop and test applications without having expensive setup for the development. (iii) Infrastructure as a service (IaaS), delivers virtual computing resources like the server, storage, hardware, software as per user's requirements.

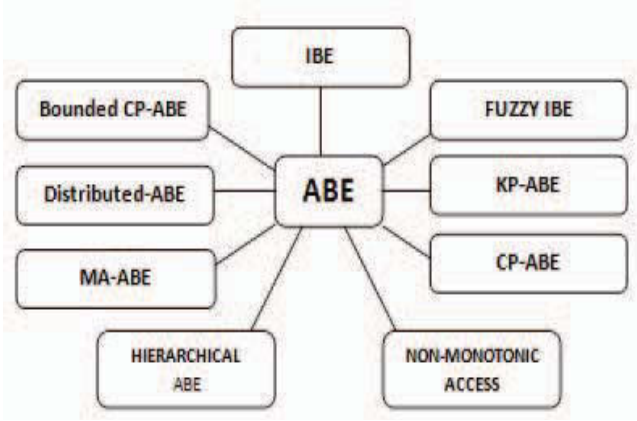

Figure 1: Types of Attribute-Based Encryption Scheme

Some symmetric and asymmetric encryption schemes are delivering strong security implementations to secure the outsourced cloud data. AES (2000) and DES (1977) are two symmetric encryption algorithms that are used to secure cloud data. AES is faster and more secure than DES. RSA (1978) is an asymmetric encryption algorithm. It is slower than AES and DES algorithms thus require higher computation cost [26].

978-1-5386-1719-9/18/$31.00

2. RELATED WORK

The comparisons are done on existing ABE schemes in [1], [13],[15]. ABE was proposed after some encroachment in Identity-Based Encryption (IBE). IBE was introduced by Shamir in 1984. In IBE Ciphertexts are associated with Identity of the recipient and to decrypt the encrypted text, that one particular attribute is accepted by the recipient's private key [4].

The fuzzy Identity-based encryption scheme was proposed by Sahai and Waters in 2005. In which the Identity is set of descriptive attributes. Identity is considered as a string of characters in previous IBE schemes. A massage can be encrypted to an identity without accessing of the public key certificate [2].

Goyal proposed a Key Policy Attribute Based Encryption (KP-ABE) in 2006. In KP-ABE, every user is assigned with an access tree structure over data attributes. In KP-ABE, a Private Key has the specification of access structure, while attributes are labeled with the ciphertexts. Leaf nodes of access tree are associated with attributes. The access structure associated with the key must be satisfied by the attributes which are related to the ciphertext for decryption [3].

Sahai, Waters and R. Ostrovsky introduced a new ABE scheme with non-monotonic access structure in 2007. This scheme permits private key of a user, to express regarding any access formula over attributes such as negative one. This feature was missing in previous ABE strategies [4]. Expression of negative attributes was not possible in previous schemes. A new ABE scheme with the capability of expressing non-monotonic access structure has introduced.

Ciphertext policy attribute based encryption (CP-ABE) was projected by Bethencourt et al. in 2007. CP-ABE system consociates the access policy with the encrypted data whereas user's private key is corresponding to the arbitrary number of descriptive attributes expressed as the string. Data owner must specify the associated access structure over attributes. Attribute of user must satisfy the access structure for decryption of the ciphertext. CP-ABE system describes the access structure as "Access Tree". The primary objective of this scheme was to achieve "collusion-resistance"[6].
This scheme eliminates the limitation of choosing the decryptor as this facility was missing in KP-ABE. However, CP-ABE has some limitations over determining user attributes and policies management. CP-ABE suffers also from the lack of efficiency and flexibility in access control [16]. An efficient user revocation scheme is also needed with proxy re-encryption scheme that will prohibit the revoked users to rejoin [17].

Melissa Chase introduced a Multi-Authority Attribute-Based Encryption (MA-ABE) Scheme in 2007. Sahai and Water proposed an encryption scheme earlier based on single authority attribute. The process of key distribution and monitoring has been improved by permitting polynomial number of attribute authorities. A data owner can select a set of attributes and a number A_k for encryption and the plain text can be encrypted in such a way that it can be decrypted only if decryptor has at least A_k of the given attributes from each authority k [5]. Each authority's attribute set to be disjoint is the main complication in MA-ABE. A fully trusted central authority (CA) is essential for this strategy, which can decrypt all ciphertexts. If CA is corrupt then it could be the biggest threat to the system.

Distributed ABE scheme was proposed by Muller in 2008. Muller introduced this scheme where attributes and corresponding secret keys are managed by an arbitrary number of parties. User's eligibility over specific attribute is verified by Attribute Authorities (AA), and if found eligible then secret attribute key is distributed to the user by AA. Boolean formula structured access policy covering some attributes is required to be computed by the user to encrypt a message in this scheme. To decrypt a ciphertext, the decryptor must retain the access to some set of attributes with their associated secret keys that will satisfy the access policy. In case of non-availability of keys, an AA can be requested to send the secret keys corresponding to attributes. This is the matter of eligibility of the user for the keys [7].

Bounded Ciphertext Policy Attribute Based Encryption scheme (BCP-ABE) was proposed by V. Goyal et al. in 2008. An access structure based on bounded size access tree was presented. This scheme has a number of theoretical assumptions based security proofs and support of advanced access structures. "Bounded Length Access Tree Threshold Gates" represents access structure as nodes in this scheme. One deficiency of this scheme is that ciphertext access formula doesn't support negative constraint representation [11].

Fine-Grained Data Access Control Encryption Scheme was proposed by J. Li et al. for securing the cloud storage [8]. Illegal key sharing is prevented among colluding users to achieve the fine-grained and secure access. An improved encryption scheme has been proposed by implementation of user accountability through the traitor tracing and definition and enforcement of access policies based on data attributes.

Data owners are allowed to execute access structure on every file so that only authorized user can access those files.

Hierarchical Attribute-based Encryption scheme (HABE) was proposed by [12]. The HIBE system and the CP-ABE system are combined to help cloud users to share their confidential data over the cloud server. They achieved full delegation, fine-grained access control and scalability with optimized performance in this scheme.

Outsourced data decryption for ABE was introduced by Green et al. in 2011. The principal aim of scheme above is to decrease the overload of the ciphertext size and computation overhead of decryption operation on user [9].
ABE with outsourced decryption scheme was introduced by Junzuo Lai et al. in 2013 [10]. This scheme eliminates the decryption overhead of the user side. The user provides a transformation key to the CSP. This transformation key can transform a ciphertext into simpler ciphertext only if the ciphertext is gratified by the user's attribute or access policy. User has to face a small computational overhead to regain the plaintext from the simple ciphertext.

RSA (Rivest-Shamir-Adleman) is an asymmetric encryption scheme. It is a very strong security algorithm technique and useful in many implementations. This scheme was proposed by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977. The idea behind this scheme is that it is very tough to factorize large integers. This algorithm is based on the theory, called "integer factorization". RSA follows the concept of one way function. This one way function is easy to compute as well as tough to compute the reverse process [23]. RSA has a complex algorithm for Public and Private Key generation. Encryption strength depends on the key size. When key size is doubled then encryption strength increases exponentially.
RSA Algorithm [25]:
Key Generation Algorithm
1. Selects two large primes randomly and secretly: x, y and compute z = x. y
2. Calculate ϕ (z) = (x – 1) (y – 1).
3. Selects Random Integer: p such as 1 <p<z and GCD (p, ϕ) = 1.
4. Calculate dk such as p. k ≡ 1 MOD ϕ(z) and 1 <k< ϕ (z).
5. Generated public Key is (p, z).
6. Generated Private Key is (d, z).

Encryption process
1. Receiver R will send his public key to sender S.
2. Sender S encrypts message M as $C = M^p |z|$ and sends C to receiver R.

Decryption Process
Receiver R decrypts the ciphertext as $M = C^k |z|$.

The main drawback of this algorithm it is slower than other symmetric encryption schemes.

AES (Advanced Encryption Standard) is a symmetric encryption scheme. This scheme was proposed by Vincent Rijmen and Joan Daemen, and U.S. National Institute of Standards and Technology (NIST) established it in 2001. Block length of 128 bytes and key lengths of 128, 192, and 256 bits are supported by AES scheme. AES is more powerful as it uses longer key size than DES or 3DES. AES-128, AES-192, and AES-256 are the three block ciphers which AES comprises. Encryption and Decryption both operations need sharing of same secret key between sender and receiver. Data is encrypted and decrypted in 128 bits using cryptographic keys of 128, 192 and 256 bits [19], [24]. AES is enough faster than 3DES (approx. 6 times) [15]. AES is the replacement of DES as it eliminates the small key size problem of DES.

DES (Data Encryption Standard) is a block cipher, means this algorithm is applied to data block-wise simultaneously rather than bitwise. To encrypt a plaintext message, DES operates on 64-bit blocks. A 56-bit long secret key used for a 64-bit ciphertext. This key size can be cracked by a brute force attack. DES is not using as a standard cryptographic algorithm because of its smaller key size problem. Same key is used for encryption and decryption process in DES. The smaller key size makes it vulnerable and this is the main drawback of this encryption scheme.

3. THEORETICAL ANALYSIS

ENCRYPTION SCHEME	PROPOSED BY	YEAR	TECHNIQUE USED
IBE	Shamir	1984	Ciphertexts associated with Identity of the recipients
Fuzzy-IBE	Sahai and Waters	2005	Having no access to a public key certificate a message can be encrypted to an identity
KP-ABE	V. Goyal et al.	2006	Ciphertext associated to sets of attributes and Private keys associated to access structures (Access Tree)
ABE with Non - Monotonic structure	R. Ostrovsky, A. Sahai, B. Waters	2007	ABE scheme with the capability of expressing non-monotonic access structure
Ciphertext policy attribute based encryption	Bethencourt et al.	2007	Arbitrary numbers of attributes are associated to private key of user. Associated access structure over attributes, must be specified by

			Data Owners.
Multi-Authority Attribute-Based Encryption	Melissa Chase	2007	Quality observation and secret key allotment is allowed through polynomial number of attribute authorities.
Distributed attribute based encryption	Muller	2008	Attributes and their corresponding secret keys are maintained by any number of parties.
Bounded - CP-ABE	V. Goyal et al.	2008	Access structure is represented by bounded size access tree-threshold gates.
HABE	Wang et al.	2010	Combined techniques of CP-ABE and HIBE system.
Outsourcing the decryption for ABE	Green et al.	2011	A transformation key has been used by cloud to convert ciphertext to simpler ciphertext.
ABE outsourced decryption	Junzuo Lai et al.	2013	Cloud may decode any ciphertext gratified by the user's attributes or access policy with a user-provided conversion key.

Table 1: ABE Schemes Technical Tabulation

In Table 1 the analysis of diverse alive encryption schemes is shown. RSA is used for encryption, decryption, digital signature generation and verification. RSA exists around us for more than 36 years and could not be easily compromised. Another advantage of RSA encryption has no extra storage overhead. It means that the size of plaintext and Ciphertext remain same in RSA encryption. Besides these qualities of RSA, it has extra computation overhead over other encryption schemes.

4. EXPERIMENTAL ANALYSIS

The authors have compared some of the existing encryption schemes on the basis of their performance against computation overhead and storage overhead. The authors have compared four encryption schemes CP-ABE, KP-ABE, RSA, and AES on variant file sizes. Table2 and Table 3 respectively show the storage cost and computation cost regarding diverse encryption schemes. Table 2 shows the storage overhead comparison among different encryption algorithms. The comparison is done on different file sizes. RSA algorithm has no storage overhead for encrypted data in comparison to other algorithms. A Ciphertext generated by CP-ABE can be associated with multiple access trees. This cause significant storage overhead on the storage server as ciphertext size grows when the number of access tree increases [29]. The ciphertext size in KP-ABE increases with the number of attributes associated with ciphertext [28]. Thus KP-ABE also suffers from storage overhead. AES increases the size of ciphertext by the padding of few bytes with the last data block. This comparison gives us the conclusion that RSA is the best algorithm for having no storage overhead.

File Size (KB) ↓	Storage cost (KB) →	CP-ABE	KP-ABE	AES	RSA
515		524	516	516	515
1026		1036	1027	1028	1026
2052		2064	2053	2052	2052
4098		4108	4099	4100	4098
8196		8208	8197	8196	8196

Table 2: Storage cost after encryption

Table 3 shows the computation cost based on same four algorithms and file sizes taken in storage cost comparison in table 2. The 2048 bits key size is used in RSA encryption. The file is divided into several fixed-size blocks of 1024 bytes.

File Size (KB) ↓	Computation cost(MS) →	CP-ABE	KP-ABE	AES	RSA
515		2439	816	735	101676
1026		2478	917	891	220094
2052		2494	1123	1147	436707
4098		2877	1766	1331	1000097
8196		3006	2532	1439	1880759

Table 3: Computation cost

In [27] the algorithm is used to improve the performance of cloud data integrity auditing setup phase through multi-threading on multi-core CPU system. CP-ABE has more computation cost than KP-ABE and AES. AES has the lowest computation cost for encryption. CP-ABE has better security concern so selecting better encryption scheme is based on the requirement. If lower computation overhead is highly required than AES would be a better solution but when security concern is high, then CP-ABE is preferred [14].

5. PROBLEM IDENTIFICATION

The authors have compared the existing encryption algorithms like CP-ABE, KP-ABE, RSA, AES based on

their storage cost and computation cost. After analyzing the authors perceived that the RSA has absorbed least storage space as compared to other encryption schemes. Further after comparing these schemes on the basis of computation cost, the authors found that the RSA has more computation cost than others. RSA algorithm is based on large integers and prime testing [25-26]. Its security is based on the difficulty of factoring large integer and for more security RSA encryption and decryption algorithm need a lot of calculation. Due to security reason, it highly requires splitting data into multiple equal size blocks [22]. The Sequential execution of RSA algorithm for the huge sequence of blocks offile results in very slow speed. To make the RSA advisable for encryption and decryption we need to optimize its cryptographic speed.

6. PROPOSED SOLUTION

The authors have proposed a solution to enhance the speed of RSA encryption for achieving lower computation overhead. This approach can be used to increase the speed of encryption, decryption of files and other RSA implementations like the signature generation or verification. The proposed solution is simply based on multithreading technique designed on multi-core CPU system. The authors have parallelized the process of encryption and decryption of a large number of data blocks. Initially, the size of block and key is 100 bytes and 1024 bits used respectively. The implementation is carried out both sequential and parallel RSA encryption systems so that results could be compared for different file sizes.

Symbol	Description
P	Large Prime Number
Q	Large Prime Number
n	Modulus for public and private key
$\phi(n)$	Totient
e	Public key Exponent
d	Private Key Exponent
E(M)	Encryption Function
M	Message
D(C)	Decryption Function
C	Ciphertext

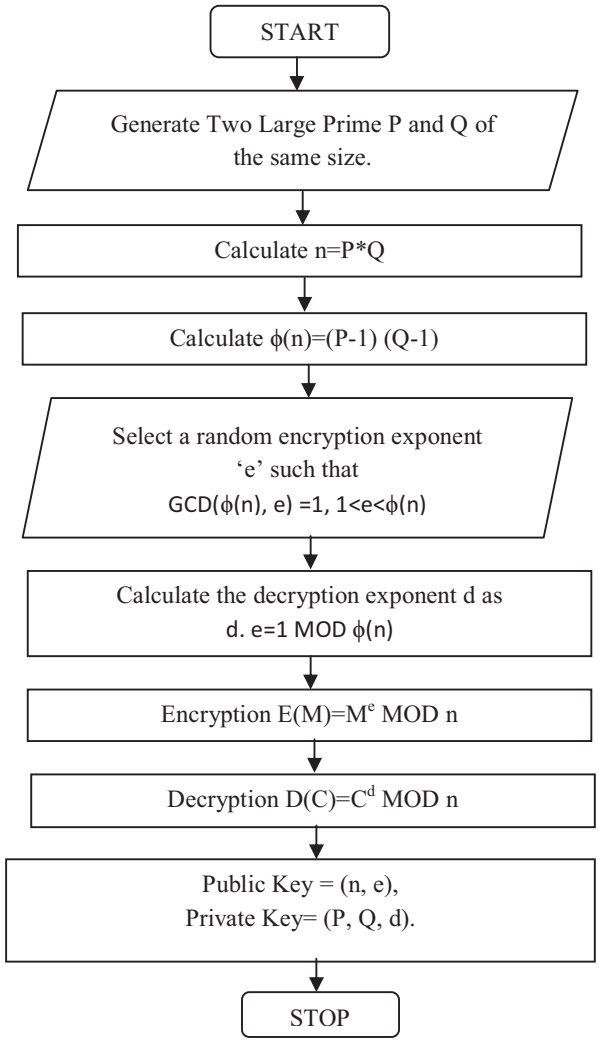

Figure 2: RSA Encryption and Decryption Flowchart

RSA Algorithm- In this approach, the file is first divided into multiple fixed-size blocks. Each block is then encrypted sequentially.

In a sequential execution, the above process of encryption and decryption is done multiple times as per the number of data blocks. The authors have implemented sequential execution of encryption process and decryption process. Both processes are performed on the Intel-based Core i3-5005U processor with 4 CPU cores. All algorithms are implemented using JAVA 8 programming language with NetBeans 8.1 IDE on windows 10 of 64-bit operating system.

Figure 3 shows the complete process of splitting, processing and joining operation performed in the ForkJoinPool framework. Work stealing technique is the major feature of this framework for improving the utilization of CPU strength. The idle worker thread can steal work from busy worker threads.

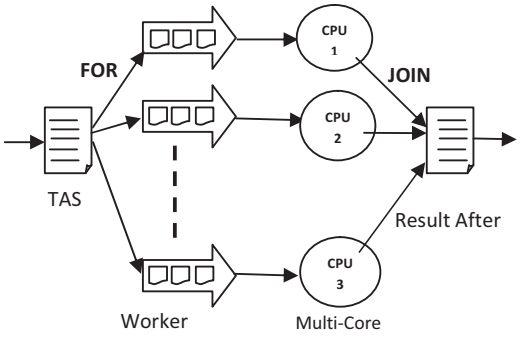

Figure 3: The ForkJoinPool Framework

7. PERFORMANCE ANALYSIS

The experiment result of comparison among different encryption schemes is shown in figure 5 and figure 6.

The algorithms have been implemented and tested for different file sizes as shown in table 4 and table 5. The sequential process of RSA encryption gives result in the high computation cost.

File Size (KB)	Number of Blocks	Encryption Time (Sec.)	Decryption Time (Sec.)
128	1311	552.04	600.62
512	5243	2615.25	2851.89
1024	10486	4262.21	4459.32

Table 4: Sequential RSA Encryption and Decryption Time

The computation cost overhead of different algorithms is shown in table 4 for encryption and decryption processes. The authors proposed a multi-threaded approach which would reduce the computation overhead and allows performing RSA encryption and decryption at highly optimized speed.

File Size (KB)	Number of Blocks	Encryption Time (Sec.)	Decryption Time (Sec.)
128	1311	21.69	34.51
512	5243	89.79	141.13
1024	10486	167.23	270.50

Table 5: Multithreaded (parallel) RSA Encryption and Decryption Time

Table 5 shows the cryptographic operation time on different file sizes on the multi-threaded model using RSA. There is a great difference between computation times of both approaches. One may seen the difference in table 6.

File Size (KB)	Number of Blocks	Encryption Time Difference (Sec.)	Decryption Time Difference (Sec.)
128	1311	530.35	566.11
512	5243	2525.46	2710.76
1024	10486	4094.98	4188.82

Table 6: Time Difference between sequential and parallel RSA

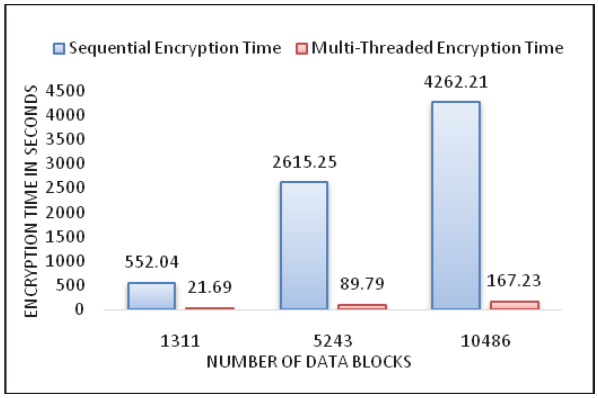

Figure 4: Comparison between the Sequential and Parallel model for computation overhead in RSA Encryption process

Figure 4 shows the difference of computation overhead of RSA encryption time for both sequential and parallel execution. Multi-Threaded (Parallel) model is much effective than the Single-Threaded (Sequential) model. The work-stealing technique improves the overall performance of the process. From figure 4 and 5, it is clear that RSA decryption is slower than encryption. Figure 5 shows the difference between sequential and parallel RSA decryption. It is proved that the proposed multi-threaded model for RSA algorithm is highly effective for reducing the computation cost. The performance of proposed approach is directly proportional to the number of available CPUs on the system.

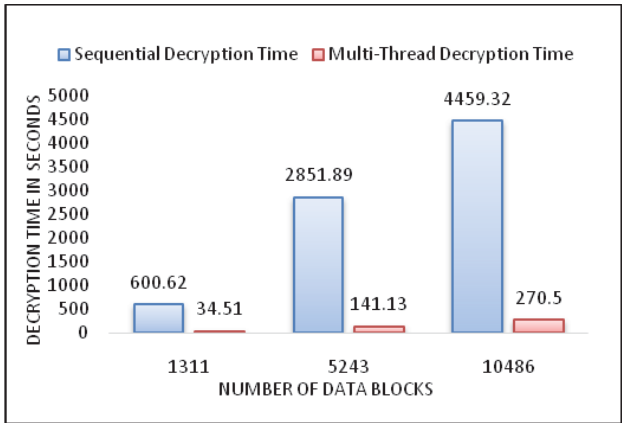

Figure 5: Comparison between the Sequential and Parallel model for computation overhead in RSA Decryption process

8. CONCLUSION

The existing encryption/decryption algorithms like RSA, AES, ABE, CP-ABE, KP-ABE and DES have been discussed in this paper with their limitations. As the yearly evolution of ABE system it becomes more secure and scalable approach for cloud computing paradigm. All the existing schemes have one or more issue of user revocation, access policy, ciphertext size, encryption and decryption overhead at data owner side. To overcome this problem of computation overhead, the authors proposed an improved RSA encryption scheme for optimizing its speed by implementing it using multi-threaded model on multi-core CPUs. The performance analysis for the aforementioned would help researchers to know about differences in sequential and parallel RSA for encryption and decryption.

REFERENCES

[1] P. G. Pawar & V. D. Thombre, "Survey Paper on CP-ABE cloud computing", International Journal of Advanced Engineering, Management and Science (IJAEMS)(Infogainpublication.com), Vol-2, Issue-12, Dec- 2016.

[2] Sahai. Amit and Brent. Waters, "Fuzzy identity-based encryption", Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 457-473, 2005.

[3] Goyal & Vipul "Attribute-based encryption for fine-grained access control of encrypted data", *Proceedings of the 13th ACM conference on Computer and communications security*, ACM, pp. 89-98, 2006.

[4] Ostrovsky. Rafail, Amit. Sahai and Brent. Waters, "Attribute-based encryption with non-monotonic access structures", *Proceedings of the 14th ACM conference on Computer and communications security*, ACM, pp.195-203, 2007.

[5] Chase. Melissa, "Multi-authority attributes based encryption", *Theory of Cryptography Conference*, Springer Berlin Heidelberg, pp. 515-534, 2007.

[6] Bethencourt. John, Amit. Sahai & Brent. Waters, "Ciphertext-policy attribute-based encryption", *IEEE Symposium on Security and Privacy,* pp. 321-334, 2007.

[7] Muller. Sascha, Stefan. Katzenbeisser & Claudia Eckert, "Distributed attribute-based encryption." International Conference on Information Security and Cryptology, Springer Berlin Heidelberg, pp. 20-36, 2008.

[8] Li. Jin, "Fine-grained data access control systems with user accountability in cloud computing", International Conference on Cloud Computing Technology and Science (CloudCom), pp. 89-96, 2010.

[9] Green. Matthew, Susan. Hohenberger and Brent. Waters, "Outsourcing the decryption of ABE ciphertext", USENIX Security Symposium. Vol. 3. 2011.

[10] Lai. Junzuo, "Attribute-based encryption with verifiable outsourced decryption", IEEE Transactions on Information Forensics and Security, 8(8), pp.1343-1354, 2013.

[11] Goyal & Vipul, "Bounded ciphertext policy attribute-based encryption" Automata, languages, and programming, pp.579-591, 2008.

[12] Wang. Guojun, Qin. Liu and Jie. Wu, "Hierarchical Attribute-based encryption for fine-grained access control in cloud storage services", ACM conference on Computer and communications security, pp. 735-737, 2010.

[13] Vinoth. C & Anantha. Raman, "A Survey on Attribute-Based Encryption Techniques in Cloud Computing", International Journal of Engineering Sciences & Research Technology 1(4), pp. 494-497, 2015.

[14] Horvath. Mate, "Attribute-based encryption optimized for cloud computing", International Conference on Current Trends in Theory and Practice of Informatics, Springer Berlin Heidelberg, pp. 566-577, 2015.

[15] Manjusha. R & R. Ramachandran, "Comparative study of attribute based encryption techniques in cloud computing", International Conference on Embedded Systems (ICES), pp. 116-120, 2014.

[16] Yu. Shucheng, "Attribute-based data sharing with attribute revocation", ACM Symposium on Information, Computer and Communications Security, pp. 261-270, 2010.

[17] Samanthula & Bharath. K. "A secure data sharing and query processing framework via federation of cloud computing", Information Systems, 48, pp.196-212, 2012.

[18] Tsai. Jia-Lun, & Nai-Wei. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services", IEEE Systems Journal 9(3), pp. 805-815, 2015.

[19] Darwazeh. Nour S, Raad S, Al-Qassas & Fahd AlDosari, "A secure cloud computing model based on data classification", Procedia Computer Science, 52, pp.1153-1158, 2015.

[20] Bera. Samaresh, Sudip. Misra and Joel. Rodrigues, "Cloud computing applications for smart grid: A survey" IEEE Transactions on Parallel and Distributed Systems, 26(5), pp.1477-1494, 2015.

[21] Hashizume. Keiko, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, 4(1), p.5, 2013.

[22] Shamir. A, "How to share a secret", *Communications of the ACM*, *22*(11), pp.612-613, 1979.

[23] Rivest. R.L, Shamir. A & Adleman. L, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol 21(2), pp. 120-26, 1978.

[24] Margaret. Rouse, "Advanced Encryption Standard (AES)", http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard, accessed online [08.july.2017].

[25] Hemalatha. S, & R. Manickachezian, "Security Strength of RSA and Attribute Based Encryption for Data Security in Cloud Computing", International Journal of Innovation Research Computation and Communication Engineering, 2(9), pp.5847-5852, 2014.

[26] Mahajan. Prerna & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for security", Global Journal of Computer Science and Technology, 2013.

[27] Deepak Kumar Verma, Purnima Gupta & Rajesh Kumar Tyagi "Optimizing the User Side Set-up Phase for Privacy Preserving Public Auditing in Cloud Storage", communicated in IGI Global, 2017(Under review).

[28] Wang. C. J & Luo. J. F, "A key-policy attribute-based encryption scheme with constant size ciphertext", *Eighth International Conference on Computational Intelligence and Security (CIS),* pp. 447-451, 2012.

[29] Guan. Z, Li. J, Zhang. Z & Zhu. L, "Conditional Ciphertext-Policy Attribute-Based Encryption Scheme in Vehicular Cloud Computing", *Mobile Information Systems*, *2016*.

Networking in IoT: Technologies used, Security Threats and Possible Countermeasures

Purnima Gupta, Aswani Kumar Singh, Archana Sharma

Abstract*: IoT is the networking of daily use objects. Internet of Things amalgamates various kinds of physical object to communicate with each other directly. These objects are commonly known as constrained devices. Constrained devices work with low memory, low storage, and low computation power. Implementing security algorithms in these devices is challenging. The researchers take these challenges as opportunity. The diverse and heterogeneous structure of the IoT phenomenon introduces a variety of new security risks and challenges. Many threats, like botnets, home intrusion, remote control of the IoT devices, and man in the middle attacks, are emerging and need a stronger security implementation to protect IoT devices from being compromised. The authors surveys different kinds of IoT networking technologies, security challenges and solutions of these challenges to form more secure IoT environment for trustful adoption of services through industrial or personal use. In this paper, the authors presented a study of numerous networking technologies along with possible threats and their countermeasures.

***Keywords*: IoT, RFID, Wi-Fi, Wi MAX, LoRaWAN, Ransomware, Botnet, APTs, Intrusion.**

I. INTRODUCTION

The Internet of Things is complex network architecture consists of variety of devices, sensors and equipment. It follows different communication protocols forming the heterogeneous devices connectivity. An IoT network refers to a collection of interconnected devices that communicate with other devices, for example, smart appliances and wearable things etc. The fundamental features of IoT networking architecture to sustain computing functionalities are scalability, availability, and maintainability. IoT is getting more attention of researchers and industries from last two decades. The main objective of IoT is the free flow of information by connecting various types of digital or physical objects having different communication protocols [1]. Devices are connected in the IoT platform through an internet connection to deliver a specific type of service using real-time communication. IoT includes communication technologies like Radio Frequency Identification (RFID), Cloud Computing, Wireless Sensor Network (WSN), Near Field Communication (NFC), Machine to Machine (M2M) Communication, Low Power Wireless Personal Area Network (LoWPAN), Worldwide Interoperability for Microwave Access (WiMAX), and others. IoT concept was initially given by Kevin Ashton in 1982 to establish an interface between human beings and the virtual environment to make their life easier [2].

The growth rate of connected devices in IoT is highly tractive today. According to an article published in Forbes, the global market of IoT growth is predicted from $157 billion in 2016 to $457 billion by 2020, attaining a Compound Annual Growth Rate (CAGR) of 28.5% [3]. The number of connected devices in IoT will grow up to 50 billion in 2020 and will surge up to 125 billion by 2030 [4].

Security vulnerabilities and cyber-attacks are more advanced and improved than before. IoT devices are widely used in electronic health monitoring systems, smart cards, home appliances, military and other types of personal or industrial objects. These devices could be vulnerable to external threats like malware, viruses, hackers, physical damages and theft. A hacker can attempt to launch phishing, SQL injection, cross-site scripting, and DDoS attacks to hack, performance downgrade or damaging devices used in IoT. Some of the popular attacks on IoT have been discussed below.

STUXNET is a malicious computer worm which affected the industrial Programmable Logic Controllers (PLCs) in Iran's nuclear-fuel enrichment project. Although STUXNET was not a type of IoT attack it was a sign that smart devices can be compromised [5]. The Mirai Botnet attack was launched to infect older routers, DVD players or IP cameras especially in 2016[6]. Mirai used these compromised IoT devices to launch the HTTP flood attack (DDoS attack) to the Dyn server. This IoT Botnet is made by Mirai malware and causes Twitter, New York Times, Netflix, GitHub, and CNN like networks to get affected by DDoS attack. The Reaper (IoTroop) was another botnet which stunned everyone in 2017, more dangerous than Mirai botnet [7]. Reaper botnet came in spotlight in September 2017 and infected over one million wireless networks. Reaper is an evolution of Mirai and uses more sophisticated hacking tools and software than Mirai. Another very harmful malware called BrickerBot came into existence and is capable of killing any unsecured IoT device. The most awful thing about BrickerBot is that consumers of IoT devices could never know that their devices are affected by this bot. BrickerBot finds an unsecured IoT device on the network and performs a series of Linux commands to corrupt the device storage or disturbs the connectivity to affect the device performance [8]. The IoT environment are still having many security loopholes. It needs a strong and trustful security mechanism to eliminate these loopholes.

Revised Manuscript Received on June 30, 2020.

* Correspondence Author

Purnima Gupta*, IT department, Institute of Management Studies Noida, Noida, India. Email: purnimaa018@gmail.com

Aswani Kumar Singh, Software Engineer, Soft-Tech development Solution, DDU, India. Email: aswanikumar124@gmail.com

Dr. Archana Sharma, IT department, Institute of Management Studies Noida, Noida, India, Email: asharma12569@gmail.com

A clear and complete structure and design of IoT is yet to define and this could be a reason that the above threats are still capable to harm devices and applications in IoT. A possible architecture for IoT is shown in figure 1.

The rest of the paper is organized in the following sections. Section 2 describes the communication strategies in IoT. In section 3, existing security threats and vulnerabilities that can harm IoT devices are discussed. Section 4 describes major technologies and mechanisms to Secure IoT. In section 5, the authors have given the summary related to the topic that can help to identify all the risks and challenges before the adaptation of IoT. In section 6, conclusions about IoT security solutions and future scope for better security is provided.

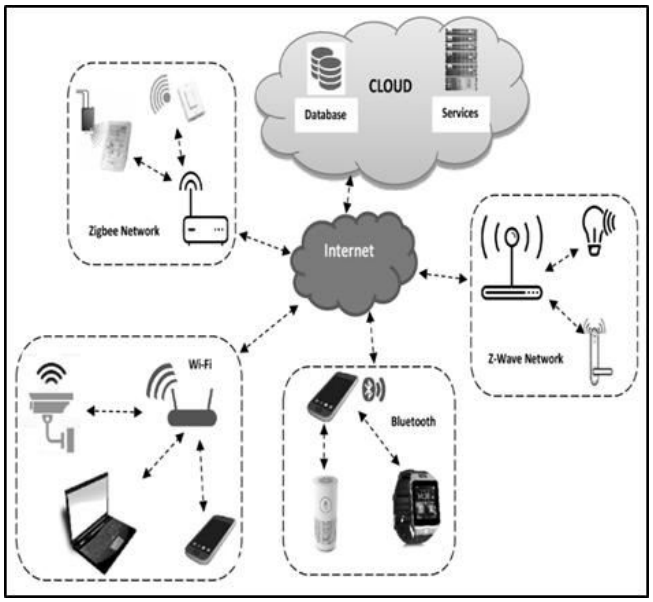

Fig.1. IoT Architecture

II. COMMUNICATION STRATEGIES IN IOT

Different networking technologies have been adopted in IoT. In this paper authors have described eight communication strategies with their operative background and architecture. Table 1 presents different IoT network architectures on different criteria like frequency, data rate and range. It also shows the vulnerabilities associated with each networking technology.

ZigBee is a low data rate, low power consumption, and low-cost wireless networking protocol used to define the operation of Wireless Sensor Networks (WSNs) and currently uses IEEE 802.15.4 MAC and PHY layers. IEEE and ZigBee combined their technological research regarding communication in devices inbuilt with Bluetooth technology and having low power and low data rate. These devices require long battery life and do not require the high-speed data rate. The range of these devices may vary from 10 meters to 75 meters. The data rates are 250 kbps at 2.4 GHz, 40 kbps at 915 MHz, 20 kbps at 868 MHz [9]. ZigBee provides interoperable data networking which operates on the upper level of the protocol stack (network Layer to application Layer). This will eliminate the consumer's dependency on product manufacturer and ensures the working between different manufacturer devices [10].

The RFID (Radio Frequency Identification) allows a computing device to read the identity of RFID tags from a distance and is a replacement of Barcode technology. RFID devices can be categorized into two classes. First is Active class, in which devices use power either from an integrated power source battery or connected to a powered infrastructure. The second class is Passive RFID which contains antenna, a semiconductor chip attached to an antenna and some form of encapsulation [11].

Table I: Different Communication Strategies in IoT

Networking Technology	Frequency (GHz)	Stream Data rate (Kbps)	Approximate Range (Meter)	Vulnerabilities
ZigBee [12]	2.4	250	150	Device tempering, key secrecy required
RFID [13]	2.45	640	100	MITM Attack, Sniffing, Denial of Service attack, Cloning & Spoofing
NFC [14]	0.13	424	0.04	Low range, Low Security
WiMAX [15]	66	126976	50000	The jamming attack, Scrambling attack, Water torture attack
BLE [16]	2.4	2048	10	Bluejacking
Wi-Fi [17][18]	5	55296	100	Vulnerable to passive attacks, Jamming and Scrambling.
6LoWPAN [19]	2.4	250	100	Low security in multi hop
LoRaWAN [20]	0.923/ 0.915/ 0.868/ 0.433	50	20000	Once hackers have the encryption keys, they can perform DoS attacks

Near Field Communication (NFC) uses magnetic field induction to establish communication among short-range and high-frequency wireless devices. NFC devices use a peer-to-peer network to perform data exchange. NFC is an upgrade to the RFID technology and has been developed by Philips and Sony jointly [21]. NFC operates in three different modes. In read/write mode interaction is made with an NFC-enabled device that reads the data from a device or writes the data to a device. In peer-to-peer mode, two-way communication is established between NFC enabled devices. In card emulation mode, the system acts as a contactless smart card [22].

Machine to Machine (M2M) system establishes direct communication between two IP-based IoT machines or sensors over wired or cellular networks to send the data to gateways or cloud servers in IoT network. Human interaction is not required for communication between devices [23].

The Worldwide Interoperability for Microwave Access (WiMAX) allows the high-speed data transfer (30-40 MBPS) and belongs to IEEE 802.16 wireless family. WiMAX is much faster than Wi-Fi and its range for connectivity and data transfer is up to 40 kilometers. Thousands of users or devices can be connected simultaneously through this network with security level implementation which lacks in Wi-Fi network [24].

Bluetooth Low Energy (BLE) uses IEEE 802.15.4 for communication between ultra-low-power IoT devices. BLE may use one of the topology formations like the tree, mesh, cluster or star for the connectivity. BLE implements frequency hopping over 37 channels for bidirectional and three channels of unidirectional [25].

IEEE 802.11 is a set of technical specifications related to communication between Wi-Fi devices. These specifications are related to the physical layer and Media Access Control (MAC) layer that connects devices like printers, scanners, smartphones, and laptops without wires. These network connections are an easy target for passive attacks. Active attacks can also be performed by exploiting hardware security loopholes and protocol vulnerabilities [26].

Low-Rate and low power Wireless Personal Area Networks (6LoWPAN) sends the data in the form of packets and uses IPv6 over the wireless network. Internet Engineering Task Force (IETF) defines the 6LoWPAN which later defines the compression and encapsulation mechanisms that enable the IPV6 over low power wireless LAN (WLAN). 6LoWPAN is being used in application areas of industrial monitoring, smart grid, general automation, home automation. 6LoWPAN utilizes the IEEE 802.15.4 to provide low layers for low power wireless network and uses 128-AES link-layer security defined by IEEE 802.15.4. IPv6 is applied to PHY and MAC layer in 6LoWPAN communications of the existing 802.15 standards [27]. LoRaWAN stands for Low Power Wide Area Network and as that name suggests, it refers to the features that support low-cost, low power, mobile communications for the IoT. It features low-power operation (around 10 years of battery lifetime), low data rate (27 kb/s with spreading factor 7 and 500 kHz channel or 50 kb/s with FSK) and long communication range (2–5 km in urban areas and 15 km in suburban areas) [28-30].

III. SECURITY THREATS AND VULNERABILITIES IN IOT

Spam is a messaging system which sends unrequested bulk messages to a target device. Spam filters are the option to identify and stop these unwanted messages. Spammers can use 2D bar codes to flood the physical site of the IoT and mislead users to reach unsolicited and unrelated content over the Internet [31]. The digital signature system can be used to overcome this problem. Mass flooding, website referrals, and Redirection hiding technique are the spamming techniques used by spammers.

Advanced persistent threats (APTs) is a type of attack in which an unauthorized user gets foothold through malware, physical malware infection or external exploitation to execute future continuous attacks for a long time period to achieve his malicious objective without being detected. There are many activities performed in this attack like network hacking, detection avoidance, determining the target area, collecting important information to gain access. This attack is basically targeted, goal-oriented, persistent and unnoticed in nature [32].

Ransomware is a type of malware that encrypts all data of your computer and sales the decryption keys to decrypt. The damage made by ransomware is irreversible and the decryption key is required for getting data back. The ransomware is a more serious threat for IoT because its action cannot be reset with our own and will have to pay for that.

Data and Identity theft could be a more serious security-related problem in the IoT. Suppose that all information got by your smartwatches, fitness tracker, GPS location data, and social media is combined together and may be sufficient to reveal your identity. Thus, identity and data theft are one of the biggest threats to the IoT [33].

Smart home corresponds to a heterogeneous network structure having a variety of devices, applications, and technologies connected together. The globally available smart home ecosystem data may prone to a security vulnerability. This electronic data needs to be protected from external intrusions which may cause several security issues like denial of service attacks [34]. Home Intrusion could be launched through several attacks like DDoS attack, Device Hijacking, and phishing (PDoS). Intrusion Detection Systems (IDS) are highly required for the safety of electronic data of a smart home. Current security measures of connected vehicles in IoT are in the poor state today. Connected remote vehicles may face several security-related issues like vehicle sensor attack, wireless carjacking, GPS Jamming and spoofing, back door attacks, front door attack, hacking of remote vehicle control application. Figure 2 has shown some of the security threats in the IoT environment. Intercepting a communication channel with malicious intention between two systems without acknowledgement of sender and receiver is called the man in the middle attack. The man in the middle attack can be launched through several techniques like Address Resolution Protocol (ARP), DNS spoofing, session hijacking, and sniffing. Once a communication channel is compromised, an attacker can hear all communication as well as can transmit false messages too. In the scenario of IoT, this attack can be more effective and saboteur. An interceptor can track your daily activities through compromised IoT devices like health monitoring system, smart cars, mobile devices, cameras, GPS navigation system and many others. Smart cars can be misguided; false health monitoring system data can be transferred to show emergency situation. A strong encryption mechanism like RSA, AES, and Blowfish can be used in IoT to get protected from this threat [35].

Radio-Frequency Identification (RFID) Skimming is the process of stealing the data or information through a chip reading device from RFID chips. Most of the new debit cards, credit cards and identity cards contain RFID chips inside them. These RFID chips use radio waves to read and capture the information from several feet away and this facility can be used to hack the RFID chips for malicious intentions. Hacked information can be used to create duplicate cards or chips and use them for illegal financial benefits.

The unencrypted data travelling to cloud interface from IoT devices can be intercepted by attackers. Cloud computing introduces potential security-related risks to IoT devices connected with the cloud. Although cloud has many strong security implementations when IoT devices with insecure credentials, unencrypted data transmission, and weak authentication mechanism connect with the cloud computing, this type of insecure connection possesses many security vulnerabilities for IoT-Cloud collaboration.

IoT devices with a mobile interface having weak or no security implementations are one of the biggest threats for the IoT.

Information can be hacked from the wearable, remote vehicle control system, remotely controlled home appliances, and other computing devices and sensors connected with an insecure mobile interface. An attacker can trace anyone's health-related information, identity, banking details easily through intercepting insecure mobile interface.

Insecure software and firmware is an easy target for botnets or malware. IoT devises firmware falls under two categories: embedded and OS-based firmware. Non-encrypted communication to the firmware of IoT devices is vulnerable to external threats like botnets. Access to these devices' firmware must be password protected and regular updates must be performed for better security. The easiest targeted devices are with default passwords. Default passwords must be changed as soon as possible to save the device from botnets and malware.

Table II: Popular Botnets with their attack techniques

IoT Botnets	Year	Attack Technique
Dark_nexus	2020	Hijacks IoT resources to carry out devastating DDoS attacks.
Mozi	2019	Used to launch distributed denial-of-service (DDoS) attacks, for data exfiltration, and for payload execution.
Brickerbot	2017	Uses exploit code to gain access and rewrite the device's flash storage with random data.
Hajime	2016	Targets devices via Telnet and gains access by brute-forcing default credentials.
Linux/IRCTelnet	2016	Sends UDP and TCP floods in both Ipv4 and Ipv6 protocols.
Mirai	2016	DDoS attacks, GRE floods and Water Torture attacks.
Bashlite	2015	Infects Linux system to launch DDoS attacks.
Wifatch	2014	Removes other malware and disables telnet access.
Aidra	2012	Telnet-based attacks on IoT devices.

IoT botnets are compromised independent internet-connected IoT devices like wearable, medical instruments, industrial systems infected with malware. These compromised devices and sensors are internet-enabled and able to transfer data automatically. Devices infection increases from one infected device to another without the knowledge of the device owner. Attackers can use these compromised devices as a botnet to launch DDoS attacks. Aidra, Bashlite, Linux/IRCTelnet, Hajime, Linux, Wifatch, Brickerbot and Mirai are some popular IoT botnets. IoT botnet is more destructive than traditional botnet and is the biggest threat for IoT network today [36]. Mirai is one of the biggest destructive botnets [37]. The first Mirai botnet attack (DDoS attack) was traced on 20 September 2016, against the website of journalist Brian Krebs at the 620Gbps.Over 24000 systems infected in this massive attack [38]. The Mozi botnet has been caught on September 2019 which relies on the distributed hash table (DHT) protocol to build a P2P network and uses ECDSA384 and the XOR algorithm. Mozi botnet uses algorithm having instruction for DDos attack, collecting bot information, execute payload on specific web address, and execute custom commands. The algorithm used to build this bot has combination of three different kind algorithms i.e. Gafgyt, Mirai, and IoT Reaper belong to malware family. it uses P2P network and there is no single point so that this bot can be eliminated completely.

Another botnet Dark-nexus is based on Mirai and Qbot and uses identical code pattern of both. Dark-nexus has same attacking technique as it launches DDoS attacks and hijacks the vulnerable IoT devices.it was built by a known botnet author for selling it online to launch DDoS attack for economical profit.

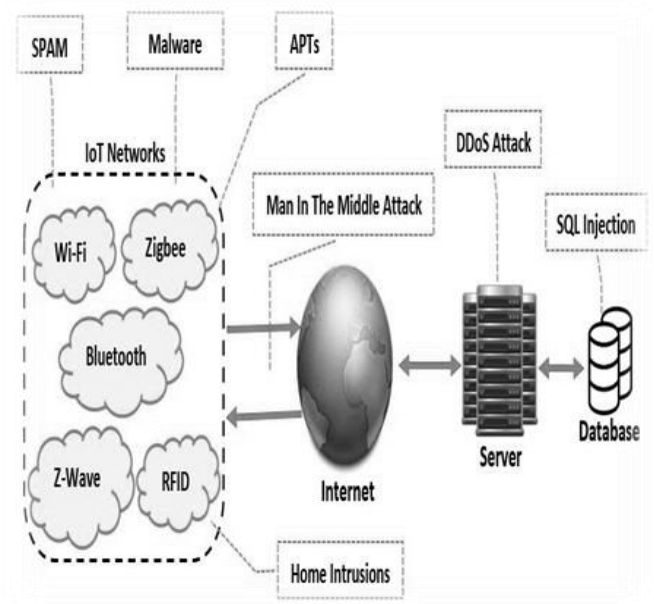

Fig. 2. Security threats in IoT

IV. SECURITY IMPLEMENTATIONS FOR IOT

IoT security threats are the major cybersecurity challenges in current IT ecosystem. In previous sections, we have discussed major IoT communication technologies and threats. Table 3 summarizes different IoT threats with their threat identity and security techniques used. A stronger security mechanism is needed to stop IoT devices from being compromised. Table 4 summarizes different network types with the security mechanism used. It's quite complex to implement stronger security to IoT devices due to their low computational capability and low memory.

Cryptography with secure encryption and decryption keys can be used to determine device identity and could make a hurdle between user data and threats. SSL certificates can play a vital role to facilitate the device identification and authentication process. Authentication process must be enforced before any software or firmware update to save IoT devices from being compromised as a botnet (Thingbot). There should be a periodic examination of the IoT network by an anti-malware utility to detect any malicious activity. Network devices like routers, printers, security cameras and other IoT devices having default passwords must be changed to a new one so that Mirai like botnets could not harm them. Spam filters can be used to stop the flood of spam. Spammers can flood the physical side of IoT devices to increase traffic for a specific page. As the problem of spamming explained in section 3, a possible solution to the spam problem is to digitally sign the 2d barcode and embedding the digital signature in QR code.

Advance Persistent Threats includes persistent behavior of attackers as they have patient until getting their target complete. Solutions to mitigate APTs may include, secure the entry point of the network, be careful to the outgoing traffic, install new security patches, and aware of any unusual activity being occurred in the network traffic.

Table III: IoT Threats and Their Security Technique

Threat Type	Threat Identity	Year	Security Technique
Advance Percistance Threats (APTs)	Monitors network activity and steal data with no damage.	2006	Beware of Trojans, suspicious emails, and malicious port scanning; install patches to prevent previously known vulnerabilities.
RFID Skimming	Stealing information from RFID cards.	2006	RFID blocking using RFID shield. Disable the RFID chip in your Credit Card.
Man in the Middle Attack	Intercepting and interrupting an interconnection between two separate network devices.	2003	Analyze the response time in the web traffic, authentication, use SSL/TLS Certificates for websites, PKI technology, WEP/WPA Encryption,
Botnet	DDoS attack	2001	Authentication, Encrypted device identity
Spam	Sends bulk messages	1994	Change passwords frequently, Web Application Firewall (WAF), DDoS mitigation system
Ransomware	Encrypts all data on the victim's computer.	1989	Data Backup, use Crypto locker software, disable RDP, and be careful when an email has a file with '.exe' extension.

Utilities like firewall, Intrusion Prevention System (IPS), Antivirus, botnet or command detection system and sandboxing should be used to ensure better security through these threats.

Table IV: IoT network security mechanisms for different network types [39]

Network Type	Security Mechanism
Zigbee	Link Layer encryption using 128bit AES, EAP, TLS.
BLE	Secure pairing
WiMAX	Sends UDP and TCP floods in both Ipv4 and Ipv6 protocols.
Wi-Fi	WEP, AES, TKIP, WPA, WPA2, and 802.1x.
6LoWPAN	Access control list, 802.15.4 link layer encryption.
NFC	Cryptographic methods and Hardware-based security (TDES, AES, RSA, ECC)
RFID	Cryptography such as Advanced Encryption Standard (AES)
LoRaWAN	AES-128 encryption, end-to-end security provided using application and network keys

The strongest possible way to save IoT from the man in the middle attack is a strong encryption system between IoT devices and communicating server of these devices. IoT devices communicate also with each other without the involvement of the server. So, encryption schemes should also be applied between IoT Devices because MITM attack is also possible between two communicating IoT devices. Another possible way to mitigate the MITM attack is by using an encrypted Virtual Private Network (VPN). This method ensures that everything comes in and goes out is encrypted and secured.

V. CONCLUSION AND FUTURE WORK

In this paper the authors reviewed and compared various existing networking technologies. Each networking technology has their own features. Authors have discussed about some prominent networking technology like Zigbee, RFID, WiMAX, Bluetooth, NFC 6LoWPAN, Wi-Fi, and LoRaWAN. The research has counter measure their scope in terms of frequency, data rate and range. The research concluded that Wi-Max has the highest frequency, data rate and network range, although Wi-Fi has also high-quality data rate and LoRaWAN has the second highest network range.
Further research has focused on authentication and access control protocols of IoT. Many researchers stated that identity of IoT devices must be secured and input-output traffic must be examined in real-time basis for any malicious activity. Devices must be protected from being compromised from malware. IoT devices need stronger security mechanisms for new emerging threats. Zigbee, LoWPAN, RFID, Bluetooth and other types of IoT networks are suffering from various types of threats like malwares, MITM attack, RFID skimming, APTs, and SPAM. Figure 3 represents the frequency comparison of different networking technologies, figure 4 provides approximate rate comparison of different networking technologies, and Figure 5 shows stream data rate comparison of different networking technologies.

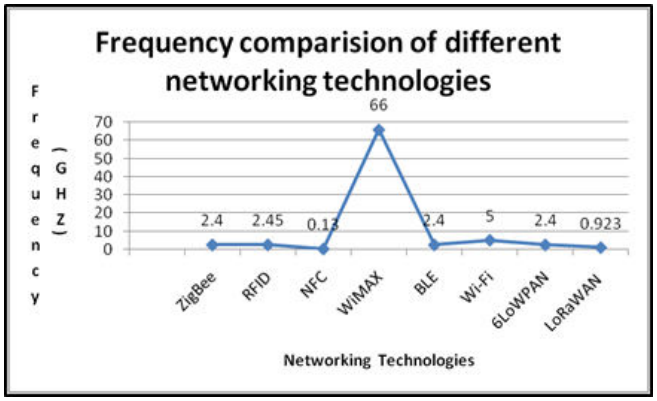

Fig.3. Frequency comparison of different networking technologies

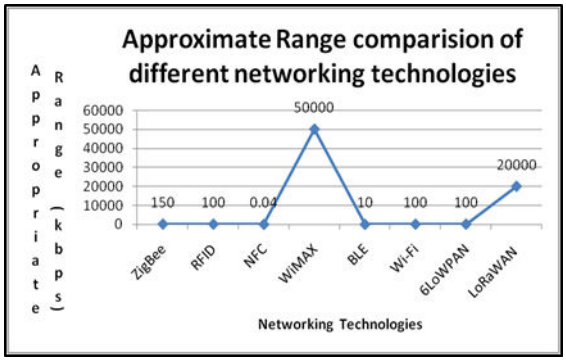

Fig.4. Approximate range comparison of different networking technologies

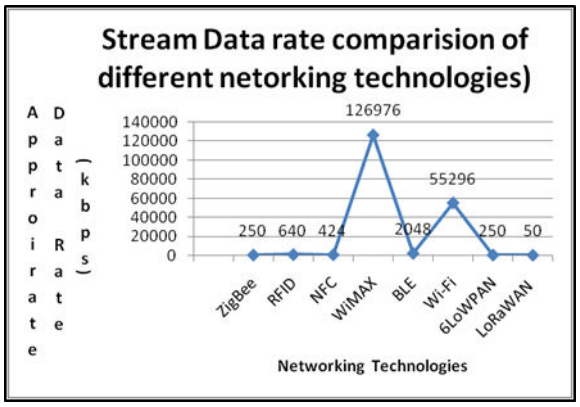

Fig.5. Stream data rate comparison of different networking technologies

The IoT framework is susceptible to attacks at each layer; hence there are many security challenges and requirements that need to be addressed. The paper illustrates the continuous attack of botnets on IoT network hence it is a biggest threat that must be included in future research on IoT security. IoT security-related challenges are getting the attention of researchers and inspire them to discover stronger security technique to mitigate these threats. Most of the IoT devices have low hardware configuration that is why the implementation of a stronger security mechanism is not possible on them. This weakness makes them vulnerable to security threats and needs further research to overcome this problem. The Internet of things reveals vulnerabilities exist in it and the requirement of research work to secure the communication between IoT device. There are several threats present which can cause damages to the IoT devices security and the world of computing has no full-proof plan or security technology to trace or eliminate these threats completely. In the end of the paper authors have presented some security mechanism to protect the networking technology.

REFERENCES

1. D. N. GUPTA, R. Kumar, and A. Kumar, "Efficient Encryption Techniques for Data Transmission Through the Internet of Things Devices," in IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks, 1st ed., V. Jain, O. Kaiwartya, N. Singh, and R. S. Rao, Eds. Pennsylvania, United States: IGI Global, 2020, pp. 203–228.
2. Shen, Guicheng, and Bingwu Liu. "The visions, technologies, applications and security issues of Internet of Things." E-Business and E-Government (ICEE), 2011 International Conference on. IEEE, 2011.
3. Howell, J. (2017, October 24). Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says. Retrieved from IHS Markit: https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says.
4. Nordrum, A. (2016, August 18). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.
5. Kushner, D. (2013, February 26). The Real Story of Stuxnet. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
6. Fruhlinger, J. (2018, March 9). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. Retrieved from CSO: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.
7. GOODIN, D. (2017, October 28). Assessing the threat, the Reaper botnet poses to the Internet—what we know now. Retrieved from Ars Technica: https://arstechnica.com/information-technology/2017/10/assessing-the-threat-the-reaper-botnet-poses-to-the-internet-what-we-know-now/.
8. Kolias, C., Kambourakis, G., Stavrou, A., &Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
9. Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.
10. Ergen, S. C. (2004). ZigBee/IEEE 802.15. 4 Summary. UC Berkeley, September, 10, 17.
11. Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. S. (2011). RFID technology principles, advantages, limitations & its applications. International Journal of Computer and Electrical Engineering, 3(1), 151.
12. Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011, April). Study on ZigBee technology. In 2011 3rd International Conference on Electronics Computer Technology (Vol. 6, pp. 297-301). IEEE.
13. Yeager, D. J., Sample, A. P., Smith, J. R., Powledge, P. S., & Mamishev, A. V. (2006, September). Sensor applications in RFID technology. In 2006 International Conference on Actual Problems of Electron Devices Engineering (pp. 449-452). IEEE.
14. Rahul, A., Krishnan, G., Krishnan, U. H., & Rao, S. (2015). Near Field Communication (NFC) Technology: A Survey. International Journal on Cybernetics & Informatics (IJCI), 4(2), 133-144.
15. Kabir, A. F., Khan, M., Hayat, R., Haque, A. A. M., & Mamun, M. S. I. (2012). WiMAX or Wi-Fi: The Best Suited Candidate Technology for Building Wireless Access Infrastructure. arXiv preprint arXiv:1208.3769.
16. Bensky, A. (2019). Short-range wireless communication. Newnes.
17. García-García, L., Jiménez, J. M., Abdullah, M. T. A., & Lloret, J. (2018). Wireless technologies for IoT in smart cities. Network Protocols and Algorithms, 10(1), 23-64.
18. Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). Emerging wireless technologies in the internet of things: a comparative study. arXiv preprint arXiv:1611.00861.
19. Al-Kashoash, H. A., & Kemp, A. H. (2016). Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering, 13(4), 268-274.
20. Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. ICT express, 5(1), 1-7.
21. Hong, Y. G., Choi, Y. H., Youn, J. S., Kim, D. K., & Choi, J. H. (2015). Transmission of IPv6 packets over near field communication. draft-IETF-6lo-NFC-00.
22. Rahul, A., Gokul Krishnan, G., Unni Krishnan, H., & Rao, S. (2015). Near Field Communication (NFC) Technology: A Survey. International Journal on Cybernetics & Informatics (IJCI), 4(2), 133-144.
23. Iqbal, M. A., Olaleye, O. G., &Bayoumi, M. A. (2017). A review on the Internet of Things (IoT): security and privacy requirements and the solution approaches. Global Journal of Computer Science and Technology.

24. Papapanagiotou, I., Toumpakaris, D., Lee, J., &Devetsikiotis, M. (2009). A survey on next-generation mobile WiMAX networks: objectives, features and technical challenges. IEEE Communications Surveys & Tutorials, 11(4).
25. Narendra, P., Duquennoy, S., & Voigt, T. (2015, October). BLE and IEEE 802.15. 4 in the IoT: Evaluation and Interoperability Considerations. In International Internet of Things Summit (pp. 427-438). Springer, Cham.
26. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879.
27. Ech-Chaitami, T., Mrabet, R., &Berbia, H. (2011). Interoperability of LoWPANs Based on the IEEE802. 15.4 Standard through IPV6. International Journal of Computer Science Issues (IJCSI), 8(2), 315.
28. Al-Kashoash, H. A., & Kemp, A. H. (2016). Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering, 13(4), 268-274.
29. Parmar, J. K., & Desai, A. (2016). IoT: Networking technologies and research challenges. International Journal of Computer Applications, 154(7), 1-6.
30. Bruce Zhou. (2017,February,9). Overview of networking technologies used to build IoT solutions. Retrieved from intelligent CIO: https://www.intelligenttechchannels.com/2017/02/09/overview-of-networking-technologies-used-to-build-iot-solutions/
31. Razzak, F. (2012). Spamming the Internet of Things: A Possibility and its probable Solution. Procedia computer science, 10, 658-665.
32. Hudson, B. (2014). Advanced Persistent Threats: Detection, Protection and Prevention. Sophos Ltd., US February.
33. D. N. Gupta and R. Kumar, “Lightweight Cryptography: an IoT Perspective,” Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 8, pp. 700–706, 2019.
34. D. N. Gupta and R. Kumar, “Generating Random Binary Bit Sequences for Secure Communications between Constraint Devices under the IOT Environment,” in INCET, 2020, pp. 1–6.
35. Cekerevac, Z., Dvorak, Z., Prigoda, L., &Cekerevac, P. (2017). INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS–SECURITY AND ECONOMIC RISKS. Journal of MEST, 5(2), 15-25.
36. Dange S., Chatterjee M. (2020) IoT Botnet: The Largest Threat to the IoT Network. In: Jain L., Tsihrintzis G., Balas V., Sharma D. (eds) Data Communication and Networks. Advances in Intelligent Systems and Computing, vol 1049. Springer, Singapore.
37. Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In Connectivity Frameworks for Smart Devices (pp. 23-41). Springer, Cham.
38. K. Angrishi, “Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets,” 2017.
39. ConstantinosKolias, G. K. (2017). DDoS in the IoT: Mirai and Other Botnets. CYBERTRUST (published by the IEEE computer society), 40-44.

AUTHORS PROFILE

Ms. Purnima Gupta is working as Assistant Professor. She has qualified 4 times UGC NET and 2 times AWES PGT exam. She has been awarded 2 times by Eastern Central Railway Pt. Deen Dayal Upadhyay Division for developing their five projects (Pension Sanitization System, Central Receipt & Dispatch Management system, LAR, RMS and TROMGS). She has done MTech (CSE) and Master of Computer Applications. She is having a rich experience of teaching and research in the field of Computer Science & Engineering. She has published and presented a large number of research papers in International as well as national journals/conferences. Her area of interest is IOT, C/C++, Compiler Design, Artificial Intelligence, Data Structure, Network Security, DBMS (Oracle/PL-SQL), HTML, CSS, Java Script, Python (Pandas, NumPy, Matplotlib) etc.

Mr. Aswani Kumar Singh is working as CMS In-charge in Indian Railways posted at ECR/DDU. He has excellent software development skills and developed lots of utilities and web interfaces to overcome many issues at East Central Railways. He has also implemented web applications developed by Center for Railways Information System (CRIS) like Accounting Management and Information System (AIMS). He has been awarded four times by Indian Railways. He has done Master in Computer Application (MCA). His research papers have been published in reputed International as well as national journals/conferences. His core interest area is JAVA, Android, SQL, Scripting Languages, CSS e.t.c. With a PhD in Computer Science

Dr. Archana Sharma has over 24 years of experience spanning the IT industry and academia in different capacities and has published 33 research papers of which 12 are in international journals. She has also authored one text book for MCA and B.Tech. students. She has organized and attended various conferences, Faculty Development Programs, workshops and seminars during her stint in different organizations and has been credited with awards and commendations. Her major areas of competencies include Advanced Database, DBMS, Distributed systems, Operating systems and C++.

Security Implementations in IoT Using Digital Signature

Purnima Gupta, Amit Sinha, Prabhat Kr. Srivastava, Ashwin Perti, and Aswani Kumar Singh

Abstract In recent advancements, different types of embedded IoT devices are connected with the wired or wireless network and continuously access the internet for communication. Cybercriminals are finding vulnerabilities on IoT devices and compromise them to launch massive attacks (e.g. DDoS, Spamming, MITM, RFID Skimming) to destroy the network. IoT devices having default authentication credentials are an easy target. To avoid cybercriminals, we need a more sophisticated authentication mechanism embedded with existing security measures. Digital signature has become an integral part of IoT to restrict illegal users. The digital signature verification process is a time-consuming operation and not advisable in IoT however we can minimize the time of verification through some optimization schemes. This paper summarizes all the existing digital signature implementation aspects in IoT and states their technological properties as well as features and loopholes.

Keywords Digital signature · IoT · DSA · ECDSA · EdDSA · BLS · RSA

P. Gupta
School of IT, IMS, Noida, India
e-mail: purnimaa018@gmail.com

A. Sinha · A. Perti (✉)
Department of IT, ABES Engineering College, Ghaziabad, India
e-mail: ashwinperti@abes.ac.in

A. Sinha
e-mail: amit.sinha@abes.ac.in

P. Kr. Srivastava
Department of Computer Science & Engineering, Dr. KNMIET, Modinagar, Ghaziabad, India
e-mail: sri_prabhat@rediffmail.com

A. K. Singh
Soft-Tech Development Solution, DDU, Bharwalia Buzurg, UP, India

M. N. Favorskaya et al. (eds.), *Innovations in Electrical and Electronic Engineering*,
Lecture Notes in Electrical Engineering 661, https://doi.org/10.1007/978-981-15-4692-1_40

1 Introduction

Kevin Ashton introduced the term Internet of things (IoT) in 1982 to establish an interface between human beings and virtually interconnected devices [1]. IoT is a network of interconnected sensors and smart network devices having different communication protocols and communication medium. IoT may include various types of networks topologies having different types of communication technologies like Worldwide Interoperability for Microwave Access (WiMax), Low Power Wireless Personal Area Network (LoWPAN), Near Field Communication (NFC), Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Wireless Fidelity (Wi-Fi). It is assumed that IoT will grow up to 50 billion devices by 2020 that will further grow up to 125 billion devices by 2030 [2]. Various applications like Smart Health monitoring, Smart Home appliances, Smart City and Smart Power Grid have millions of devices and generate a massive volume of data. Sensors are used to monitor various physical conditions like temperature, sound, pressure, light, speed, etc. Fig. 2 shows the basic structure of IoT.

IoT devices use the internet for communication hence vulnerable to external threats. Cybercriminals can attack the IoT device and use them as a bot. Further, these devices can be used as botnets to destroy communication of a victim network. Botnets are major threats for IoT. Botnets are nothing but compromised internet-connected IoT devices. Attackers can use these compromised devices as a botnet to launch DDoS attacks. Aidra, Bashlite, Linux/IRCTelnet, Hajime, Linux, Wifatch, Brickerbot and Mirai are some popular IoT botnets. Hajime is one of the IoT botnets who target IoT devices via Telnet and gains access by brute-forcing default credentials. Although defaults credentials of devices like routers must be changed before use, however, this could be ignored. These devices are an easy target for cybercriminals. TLS, SSL and Digital Signature Certificate standards can be used for security from such threats [3–6].

Digital signatures are gaining legal acceptance over the traditional hand-written signatures. it works on public-key cryptography which is designed to protect the genuineness of a digital document. Digital signature schemes have been proposed to get overcome the security problems in authentication, confidentiality, and Integrity related problems in IoT. Many digital signature schemes have been proposed earlier like RSA, DSS, and Al-Gamal digital signature schemes. Using a digital signature for a secure authentication process would certainly prevent the IoT devices to be compromised easily. Figure 1 represents the base model of the digital signature algorithm. The digital signature is proof that the coming message or command is from an authentic source [7–11] (Fig. 2).

This paper has been divided into eight sections. Section 1 represents the basic structure of the IoT and the requirement for the digital signature has been found for security-related issues. Section 2 explains the related work done previously by the researchers to implement digital signature algorithms like RSA, DSA, EdDSA, Short Signatures (BLS) including their algorithms. Section 3 represents the latest digital signature implementation with its technical introductions. Section 4 demonstrates the

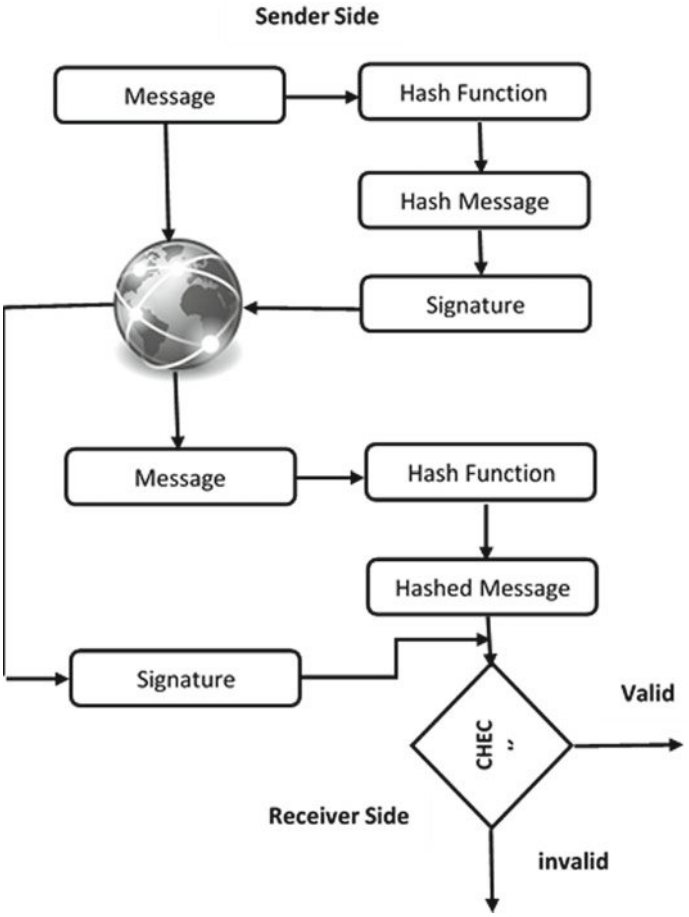

Fig. 1 Digital signature model

problem statement. Sections 5 and 6 represent the proposed solution and performance analysis details respectively. Section 7 summarizes the findings of the paper, as well as Sect. 8, which holds the conclusion about this survey paper.

2 Related Work

2.1 RSA Based Signature Scheme

The method which uses public-key cryptography, developed by Rivest, Shamir and Adelman in 1977 is known as RSA. A digital signature scheme with public-key

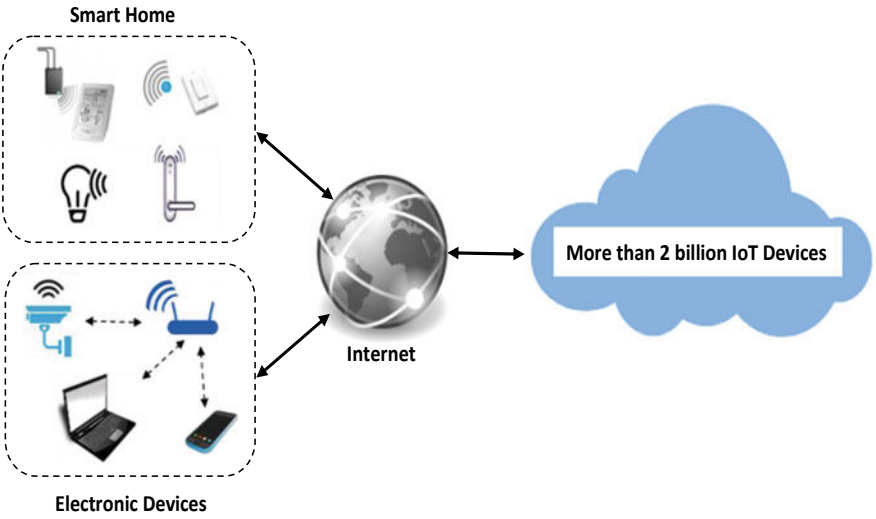

Fig. 2 Internet of things (IoT) basic structure

cryptography has been introduced in 1976 by Whitfield Diffie and Martin Hellman. Sender's private key is used to create an RSA digital signature. RSA based digital signature scheme has two basic steps [12].

- Signature generation through the private key of the signer.
- Message verification through the corresponding public key.

A signature generated by the first step will always verify the second step. Old RSA implementations are vulnerable to some attacks. Dan Boneh and others identified an attack on RSA. This attack was based on doing faulty calculations. The private key can be obtained from the faulty signatures by injecting random faults in RSA calculation. For protection from the Fault Based Attacks, Mihir Bellare and Phillip Rogaway suggested two provably secure scheme for RSA in 1996.

- The Optimal Asymmetric Encryption Padding (RSA-OAEP)
- The Probabilistic Signature Scheme (RSA-PSS)

Encryption and decryption functions are inverse of each other for RSA public/private key triple (e, d, n).

$$\begin{aligned} \text{Public key } f(m) &= m^e \mod n \\ \text{Private key } g(m) &= m^d \mod n \end{aligned}$$

Then,

$$f(g(m)) = m \text{ and } g(f(m)) = m$$

RSA-PSS is now able to handle Fault Based Attacks by encoding random values in the signature. Those random values could not be extracted from the signatures. Coron and Mandal have also proved that it is impossible to get the private key through fault-based attacks [13].

2.2 Digital Signature Algorithm (DSA)

A DSA digital signature is generated using some set of parameters like data that requires to be signed, private key 'x', secret key 'k' per message, and hash function. The same digital signature can be verified using the same domain parameters and public key 'y', data to be verified and the same hash [14].

Components of Global Public-Key

- 'P'- A prime number of n bits where n is a multiple of 64 and $512 \leq n \leq 1024$
- 'q'- A 160-bit prime factor of p–1
- 'g'- $= h(p–1)/q \bmod p$, where h is any integer with $1 < h < p–1$, such that $(h(p–1)/q \bmod p) > 1$

Private Key
'x' is a random or pseudorandom integer with $0 < x < q$.

Public Key
'y' $= g^x \bmod p$

Secret Key
A random or pseudorandom integer with $0 < k < q$.

Sign

$$\begin{aligned} r &= \left(g^k \bmod p\right) \bmod q \\ s &= \left[k^{-1}(H(M) = xr)\right] \bmod q \\ \text{Signature} &= (r, s) \end{aligned}$$

Verify

$$\begin{aligned} w &= \left(s'\right)^{-1} \bmod q \\ u1 &= \left[H\left(M'\right)w\right] \bmod q \\ u2 &= \left(r'\right) w \bmod q \\ v &= \left[\left(g^{u1} y^{u2}\right) \bmod p\right] \bmod q \\ \text{Test}: v &= r' \end{aligned}$$

2.3 Elliptic Curve El-Gamal Digital Signature Scheme

Taher El-Gamal was the first mathematician who proposed a public-key cryptosystem based on a discrete logarithm problem (DLP). ECDSA is a variant of RSA and DSA. It offers the small key size as well as significant improvements in the generation and verification timings with the small requirement of bandwidth, processing capability, and storage space. This digital signature scheme has the same form as the public key and private key.

Key Generation

- Entity T selects a random integer k_a from the interval [1, n–1] as a private key.
- the public key is computed as $T = k_a\ G$.
- The public key is stored on the public key server.

Signing Scheme

- Random integer k is selected from the interval [1, n–1].
- Computes $R = kG = (x_R, y_R)$ where, $r = x_R$ MOD n, if $r = 0$ then go to step 1.
- Compute $e = h(M)$, where h is a hash function $\{0, 1\}^* \rightarrow F_n$.
- Computes $s = k^{-1}(e + rk_T)$ mod n; if then go to step 1 (R, s) is the signature message.

Verifying Scheme

- Verify that s is an integer in [1, n–1] and $R = (x_R, y_R) \in E(F_q)$.
- Compute $V_1 = \mathrm{sR}$.
- Compute $V_2 = h(M)\ G + rT$, where $r = x_R$
- Accept only if $V_1 = V_2$.

Elliptic curve ciphers require less computation power, communication bandwidth memory and require a high level of mechanical abstraction for abstraction. Cryptographic implementation in smaller chip sizes is highly required the ECDSA to reduces the heating problem in chips and power consumption [15].

2.4 Edwards-Curve Digital Signature Algorithm (EdDSA)

This signature scheme is a variant of Schnorr's signature system with (possibly twisted) Edwards curves which provides high performance on a variety of platforms. EdDSA does not require the use of a unique random number for each signature. It is more effective for side-channel attacks and hash function collisions do not break this system hence it is collision resilience [16].

Key Setup

- Compute $H(k) = (h_0, h_1, \ldots h_{2b\text{-}1})$.
- $a = (h_0, \ldots, h_{b\text{-}1})$.
- $b = (h_b, \ldots, h_{2b\text{-}1})$.
- Compute public key $A = aB$.

Signature Generation

- Compute ephemeral key $r = H(b, M)$.
- Compute ephemeral public key $R = rB$.
- Compute $h = H(R, A, M)$ and convert to integer.
- Compute $S = (r + ha) \bmod l$.
- Signature pair is (R, S).

Verification Stage

- Compute $h = \text{hash}(R + A + M) \bmod q$
- Compute $P1 = s*G$
- Compute $P2 = R + h*A$
- Check if $P1 == P2$

The signing and verification process of EdDSA is simpler, faster and more secure than ECDSA. Unlike ECDSA the EdDSA signatures do not provide a way to recover the signer's public key from the signature and the message [17].

2.5 Short Signature Scheme

A short signature is about half the size of the DSA signature with the same level of security and promisingly used in the low-bandwidth communication environment. RSA, DSA, and ECDSA provide relatively long signature which is undesirable [19, 20]. The short signature scheme provides 160-bit signature length which is the smallest among signature sizes produced by RSA, DSA, and ECDSA. BLS based short signature scheme has been proposed by Boneh et al. in 2001 [18]. Bilinear pairing 'e' and elliptic curve group elements as signatures are the components of BLS signature [21].

Key Generation
Select a number x as your private key in the range [0, r-1]. The public key shared is g^x.

Sign
Given the private key x and some message m, the signature is given by
$(H(m))x$.

Table 1 Advantages and disadvantages of some widely used digital signatures [22]

Signature scheme	Advantage	Disadvantage	Signing speed
RSA	• Fearless key distribution • Large networks have a smaller number of keys	• Slow operation • High computation cost • Vulnerable to multiplicative attacks	Slow
DSA	• Short signature length • Lower signature computation time • Less storage requirement	• Signature verification must have complicated remainder operators	Moderate
ECDSA	• No application performance issues • Fast signing and verifying process • Support for national information protection standards	• A chance of error that makes it possible to select a private key value and identical signatures for different documents can be obtained • Requires a random number per signature	Moderate
EdDSA	• High speed • High performance • Independence of the random number generator	• Can be hacked by large quantum computers	Fast
BLS [23]	• Short signatures • Better performance • Simplified computing • No need for random number • Many signature blocks can be combined into a single signature	• Pairing is hard and not efficient • Security proof is hard	Fast

Verify
To verify that the signature is valid, we check that

$$e((H(m))x,\ g)\ =\ e(H(m),\ gx),\ \text{given}\ gx,\ g.$$

The major drawbacks of the short signature scheme (BLS) are pairing is hard as well as inefficient and security proof generation is also harder than other algorithms (Table 1).

3 Digital Signature Schemes in IoT

Digital signatures are getting used in e-commerce, banking, software systems, and an effective technique to verify authenticity and non-repudiation of the message. All these sectors have versatile computing devices connected through a network, need

Table 2 Different digital signature schemes implemented in IoT for security

Digital signature scheme	Year	Proposed by	Technique used
Shortened Complex Digital Signature Scheme (SCDSA) [24]	2018	Mughal, M. A., Luo, X., Ullah, A., Ullah, S., & Mahmood, Z.	A lightweight Shortened Complex Digital Signature Algorithm (SCDSA) for providing secure communication between smart devices in human-centered IoT
Lamport Signature Scheme [25]	2018	Abdullah, G. M., Mehmood, Q., & Khan, C. B. A.	Lamport signature scheme, which is quantum-resistant, for authentication of data transmission and its feasibility in IoT devices.
Proxy Blind ECDS Algorithm [26]	2018	Harini N, Kamakshi Devisetti R N, Aruna D	Elliptic Curve Cryptography (EEC) based on proxy blind signing procedure
Cloud-Based Digital Signature Application [27]	2018	Sahar A. El-Rahman, DaniyahAldawsari, OmaimahAlrashed, Ghadeer Alsubaie	a digital signature mobile applicationwhere it provides a cloud-based digital signature with high security to sustain with the growth of IoT.
Elliptic Curve Digital Signature Algorithm [28]	2016	B. Sindhu, R. M. Noorullah	Used the standards of the Elliptic Curve digital signature scheme.

a very strong authentication scheme to verify the identity proof and genuineness of transmitted data. Many digital signature schemes have been proposed by researchers to mitigate the security-related vulnerabilities in IoT.

In Table 2, we have illustrated some newest digital signatures with their technical summary. These digital signature techniques certainly deliver us new improved algorithms that provide better security than earlier algorithms. Still, these digital signature algorithms need to be verified for their hidden drawbacks to present an improved and completely secure Internet of Things network. This improvement is also necessary to make its users fearless about security-related risks in IoT.

4 Problem Statement

Secure communication is the key requirement between two communicating IoT devices. The owner of the IoT network may need to upgrade the firmware of IoT devices to deploy some security patches. It is to be ensured that data transmission is to be done within a secure and authenticated environment.

In many cases, cybercriminals may compromise the communicating device and use them as a lot to launch future attacks to harm a specific target system. Patching or executing a malicious program can lead to severe damages or losses if the device is deployed in a critical environment such as smart power grids, nuclear facilities, traffic management systems or flight management systems. So, this is highly required to verify the authenticity of the receiver before transferring the confidential data or installing the important patches.

There are several digital signature schemes such as DSA, ECDSA, EdDSA but the problem with these cryptographic signatures they are very much insecure and vulnerable to be broken by a quantum computer [10]. There should be a stronger, complex and unbreakable algorithm for the digital signature scheme so that the security of IoT devices can be ensured.

5 Proposed Solution

An existing digital signature system must not vulnerable to attackers. An attacker can launch Fault Based Attacks and Bleichenbacher Attack in old RSA based digital signature schemes to obtain the private key. RSA-PSS may be a solution to this attack. It has been proven that the signature generated by RSA-PSS could not let the attacker extract the private key. Performance-related issues can be minimized using batch processing and multithreading approaches.

ECDSA has less impact over EdDSA and is a newer technology than EdDSA. EdDSA provides high performance on platforms and does not need a random number for each signature. It is enough strong against side-channel attacks. EdDSA provides collision resilience, meaning that hash-function collisions do not break this system. Table 1 presents that EdDSA is the best select digital signature scheme on various factors like performance, complexity, and speed. EdDSA has minimum disadvantages among DSA, RSA, ECDSA, BLS based short signature schemes. This digital signature scheme is desirable in the IoT network for the protection of the authenticity of messages. The only drawback of the EdDSA scheme found that it can be hacked through large quantum computers.

6 Performance Analysis

DSS is considered to be stronger than El-Gamal since in this scheme the secret number k is harder to obtain from r because of the reduction mod q. The verification step in DSS is also faster than the corresponding step in El-Gamal, since there are fewer modular exponentiations to perform, and this is an important practical consideration. Performance analysis shows the RSA has the worst performance regarding signature generation time (7.8 ms) and BLS has the worst performance in the signature verification phase (0.8.6 ms). The outcome of this paper can affect the selection

Table 3 Digital Signature Schemes characteristics

Signature scheme	Key size (bits)	Signature size (bytes)	Signature generation time (ms)	Signature verification time (ms)
RSA	1024	128	7.8	0.4
DSA	1024	384	3.5	4.5
ECDSA	160	64	3.1	8.2
EdDSA	256	512	0.08	0.16
BLS	100	20	2.2	8.6

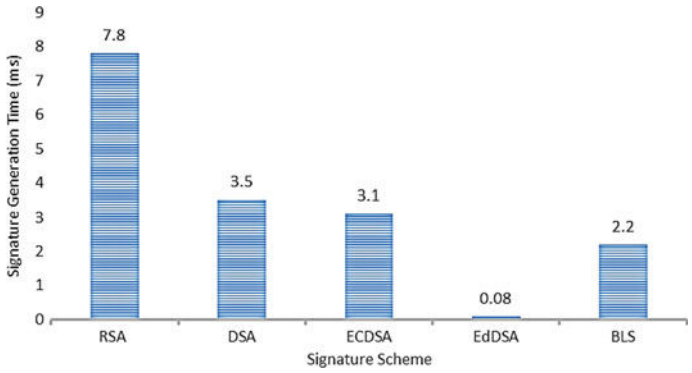

Fig. 3 Digital signature generation time comparison

of the digital signature scheme of the sophisticated software network system seeking security-related issues (Table 3).

Performance analysis has been done on various factors like key size, signature size, signature generation time, and signature verification time. EdDSA has the minimum signature generation time (0.08 ms) and signature verification time (0.16 ms) having 256 bits of key size and 512 bytes of signature size. Figure 3 demonstrates the chart of signature generation time comparison and Fig. 4 displays the signature verification time comparison for all five selected algorithms.

7 Conclusions

The meticulous survey of the different digital signature schemes reflects their advantages in terms of performance, correctness, complexity, suitability in IoT platform and stability against security threats found as a major challenge for IoT network. Performance improvement is the key challenge in implementing digital signature in IoT. This survey opens up the need for a detailed study of practical threats and related

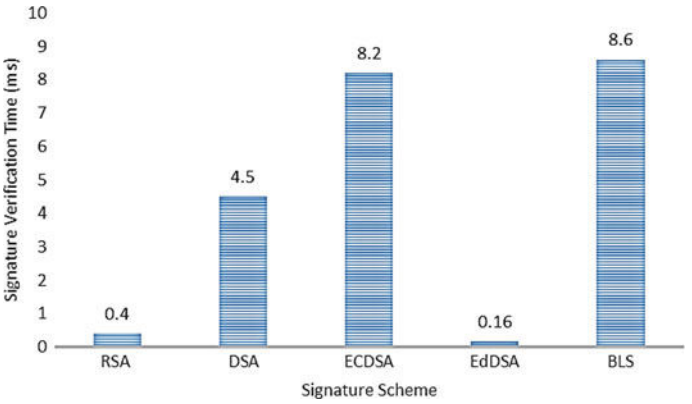

Fig. 4 Digital signature verification time comparison

analysis. This can help create a generic, concrete and usable authentication scheme based on the digital signature.

8 Summary

Authors have analyzed different types of digital signature schemes like EdDSA, RSA based digital signature, Lamport Signature Scheme, and Secure Proxy Blind ECDS. The working technique, advantages, security strength with limitation and drawbacks have been discussed briefly. A few problems of existing digital signature schemes for securing the IoT network have been identified like performance, complexity, and storage related. Authors find EdDSA has the top performance regarding the signature generation and verification processes. EdDSA can be adopted for IoT as the optimized digital signature scheme. RSA signature can be selected if the signature generation is getting performed on the client-side. This will certainly affect the server performance as the signature verification process takes minimal time among all five selected and benchmarked digital signatures.

References

1. Ashton K (2009) That 'internet of things' thing. RFID J 22(7):97–114
2. Hajkowicz SA et al (2016) Tomorrow's digitally enabled workforce: megatrends and scenarios for jobs and employment in Australia over the coming twenty years. Australian Policy Online
3. Zhang W (2010) Integrated security framework for secure web services. In: 2010 third international symposium on intelligent information technology and security informatics. IEEE
4. Geer D (2003) Taking steps to secure web services. Computer 36(10):14–16
5. Stallings W et al (2012) Computer security: principles and practice.: Pearson Education, Upper Saddle River, NJ, USA

6. Hiltgen A, Kramp T, Weigold T (2006) Secure internet banking authentication. IEEE Secur Priv 4(2):21–29
7. Kardi A, Zagrouba R, Alqahtani M (2018) Performance evaluation of RSA and elliptic curve cryptography in wireless sensor networks. In: 2018 21st Saudi computer society national computer conference (NCC). IEEE
8. Hassan, R, Toheed Q (2010) Asymmetric-key cryptography for Contiki. MS thesis
9. Wong, CK, Lam, SS (1998) Digital signatures for flows and multicasts. In: Proceedings sixth international conference on network protocols (Cat. No. 98TB100256). IEEE
10. Rabah K (2005) Elliptic curve ElGamal encryption and signature schemes. Inf Technol J 4(3):299–306
11. Stallings W (2013) Digital signature algorithms. Cryptologia 37(4):311–327
12. Kenneth L (2013) Digital signatures using RSA. mathematical sciences UMass Lowell [Online]. Available: http://faculty.uml.edu/klevasseur/math/RSA_Signatures/RSA_Signatures.pdf
13. Coron J-S, Mandal A (2009) PSS is secure against random fault attacks. In: International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg
14. Barker EB (2009) Digital signature standard (DSS). No. Federal Inf. Process. Stds. (NIST FIPS)-186-3
15. Imem AA (2015) Comparison and evaluation of digital signature schemes employed in NDN network. arXiv preprint arXiv:1508.00184
16. Nakov S (2018) EdDSA and Ed25519 [Online]. Available: https://cryptobook.nakov.com/digital-signatures/eddsa-and-ed25519
17. Samwel N et al (2018) Breaking ed25519 in wolfssl. In: Cryptographers' track at the RSA conference. Springer, Cham
18. Boneh D, Lynn B, Shacham H (2004) Short signatures from the Weil pairing. J Cryptol 17(4):297–319
19. Sethi A, Vijay S, Saini JP (2018) Analytical Model for Secure Pairing in ad hoc Network. In: 2018 IEEE 3rd international conference on computing, communication and security (ICCCS). IEEE
20. Tso R, Okamoto T, Okamoto E (2009) Efficient short signatures from pairing. In: 2009 Sixth international conference on information technology: new generations. IEEE
21. Srikar V (2018). The BLS signature scheme-a short intro [Online]. Available: https://medium.com/chain-intelligence/the-bls-signature-scheme-a-short-intro-801c723afffa
22. Zhanna L (2018). A guide to digital signature algorithms [Online]. Available: https://dzone.com/articles/digital-signature-1
23. Stepan (2018) BLS signatures: better than Schnorr. Crypto Advance [Online}. Available: https://medium.com/cryptoadvance/bls-signatures-better-than-schnorr-5a7fe30ea716
24. Mughal, MA et al (2018) A lightweight digital signature based security scheme for human-centered Internet of Things. IEEE Access 6:31630–31643
25. Abdullah, GM, Mehmood, Q, Khan, CBA (2018) Adoption of Lamport signature scheme to implement digital signatures in IoT. In: 2018 International conference on computing, mathematics and engineering technologies (iCoMET). IEEE
26. Harini N, Kamakshi D, Aruna D (2018) Secure proxy blind ECDS algorithm for IoT. Int J Pure Appl Mathe 118(7):437–445
27. El-Rahman, SA, et al (2018) A secure cloud based digital signature application for IoT. Int J E-Ser Mobile Appl (IJESMA) 10(3):42–60
28. Sindhu B, Noorullah RM (2016). Secure elliptic curve digital signature algorithm for internet of things. Global J Comput Sci Technol