Innovations

Importance of security features during online web surfing

Rishi Shukla[1], Prem Kumar Gautam[2], Manjusha Tiwari[3], Hemant Kumar[4] and Vipin Saxena[5]

[1,2,3]Department of Law, Ram ManoharLohia National Law University,Lucknow, Uttar Pradesh 226012, India

[4,5]Department of Computer Science, Babasaheb Bhimrao Ambedkar University, VidyaVihar, Rae Bareli Road, Lucknow, Uttar Pradesh 226025, India

Corresponding author: **Rishi Shukla**

Abstract: *Due to the rapid growth of cloud servers, millions of users have connected across the globe, and users are increasing in an exponential manner for the use of internet services provided by various organizations in the form of private or public clouds. Amazon, Google clouds are widely used across the globe by the users. Recently, the technology is rapidly changing through reduction in chip sizes of the devices, increment in the memory size in terms of terabytes and reduction of the overall cost involvement of the devices, many of the organisations have shifted the business over the cloud servers, where the cost of the storage space is to be paid by the organizations. Organizations have now allowed to the employees that business can be done from the home. On the other hand, due to Covid-19, online education to the children has also gained the popularity which is based on the maximum number of students in low price. Without the movement of the user from one place to another place, all kinds of work available over the cloud servers, can be easily handled. This is the beauty of the approach of distributed computing. In the present article, importance of various security features which are to be followed by the authorised user when doing online surfing. This may include seeing the website, passing the information in the form of text audio, video form, transacting the digital currency/e-cash/crypto currency through credit or debit cards, and many more. Generally, users are unaware from the hackers/intruders who are hacking the user's information over the online network and misusing the information to steal digital currency/e-cash/crypto currency or important information. The goal of this article is to fill these gaps in order to raise the user awareness when surfing the web pages through high speed internet connectivity. Obviously, the present work shall minimize the rate of cyber-crimes.*

Keywords: *Cloud Server, Information, User, Internet and Privacy*

1. Introduction

As the hand-held devices like mobile, smart phone, smart watch, laptop, tablet, palmtop, etc. are well connected across the cloud servers which is rapidly growing in a distributed manner and through said devices, daily interactions across the network are tremendously increasing. However, the privacy of individual user is at the risk due to involvement of digital currency/e-cash/crypto-currency which is to be transferred by the user over the network from one device to another device. Further, world-wide it is observed that accessing of the cloud servers by the users are increasing day by day. From the literature, it is found that only 21% Indian users were using the internet services in the year but due to tremendous growth of the hosting of the websites over the cloud servers by various organizations, there is tremendous increment of the users to use the internet services and hence presently around 61% users of

total Indian population are using the internet facilities available through the cloud servers as depicted through the following figure1.

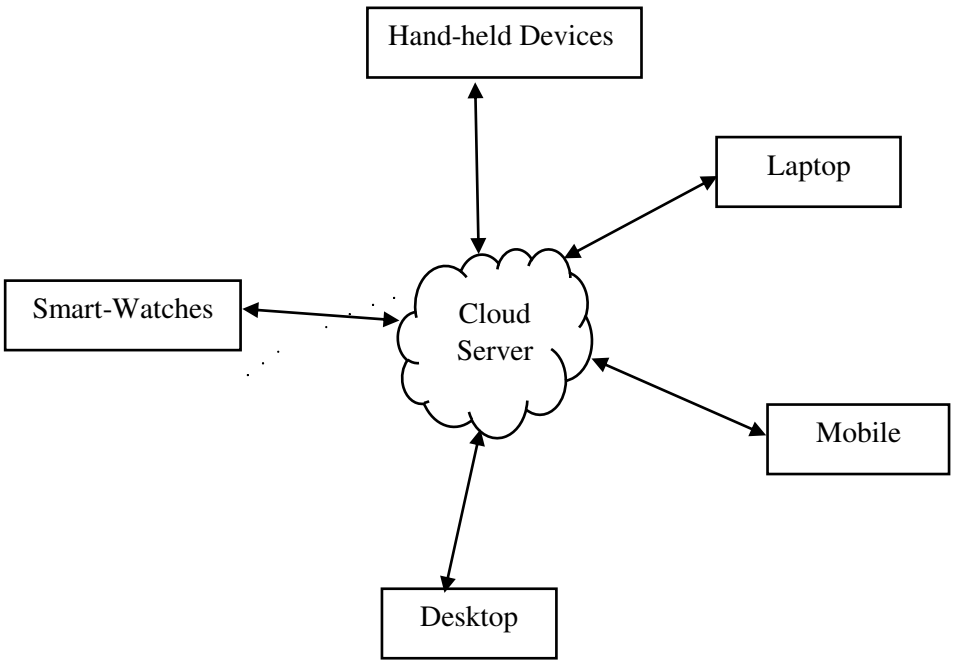

Figure 1.Accessing of Cloud Server by various Hand-Held Devices

Generally, the users are using the various devices for accessing the cloud servers through internet facilities available either through mobile data or through wi-fi network services. The duplex connection among the devices is represented in the above figure. Let us describe various kinds of the services offered by the cloud servers and provided by the various organizations in the form of private or public clouds. The services may be shopping, accessing of virtual library, hospitals, government organizations, companies, banking sector, insurance sector, on-line gaming etc. The shopping by the users may be done through various clouds like Amazon, various websites available under Google clouds and many more. Generally, these clouds provide the facility to the user for initial registration by entering the mobile device number, unique identification of the country but from the literature, it is again seen that many of the intruders and hackers are performing online crimes by entering the fake identification number and also the mobile number associated with another one. The various kinds of the services provided by cloud servers are shown in the following figure 2.

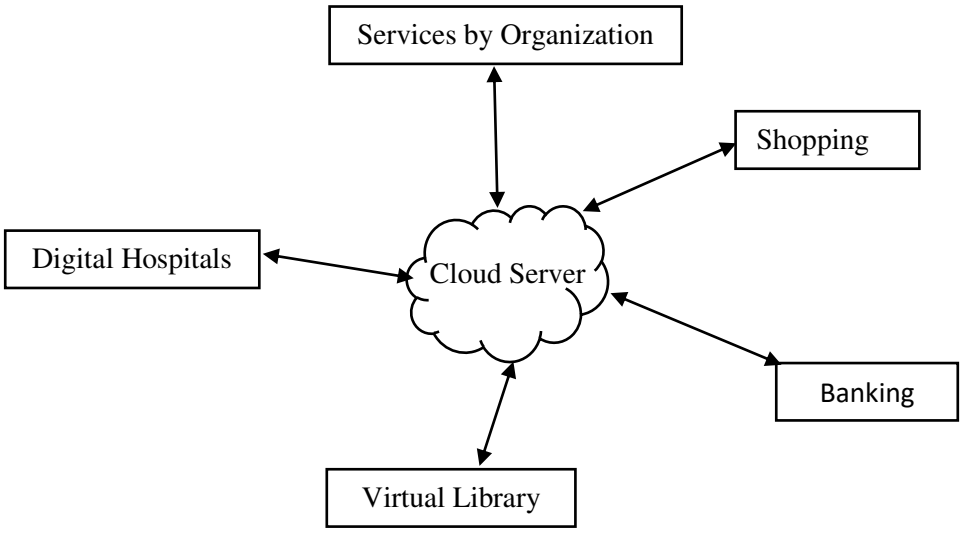

Figure 2 Services provided by Cloud Servers

Frome the literature, it is revealed that the developed countries in comparison of developing countries are having the more percentage rate of the users who are using the internet services and accessing the cloud services, for example United State of America(USA) has 95.5% of users from total population who are using internet facilities while country like China, only 71% users of total population are using the internet services. The reasons for increasing the accessing of internet services are promotion of online education, sales and purchases, work from home, social networking, shifting of companies over cloud servers and many more. Still around 39% users of total Indian population are not using internet facilities but users are increasing day by day. For the, users who are using the internet facilities through cloud servers, it is necessary to understand the security features when surfing over the web. It is must for secure access of cloud servers in such a way that hackers/intruders could not be able to perform cyber-crime but before description of important security features, let us describe some of the important research work available in the literature in the subsequent section.

2. Related Work

Frome the literature, it is revealed that scientists and engineers are continuously working on the safe and secure online transaction and developing the various methods and algorithms from time to time. Milenkovic [1] is an important source of the information in which distributed security algorithms are available which can be used for transaction of data over the cloud servers which are interconnected by means of dynamic network topological structures [2]. For development of various kinds of security algorithms, one must have thinking power to develop the logic with strong mathematical background. Hackers and intruders are watching the online surfing of the various users. When one transacts high value of currency for any purpose over the internet, then there is need of high-level security. For this purpose, Rivest, Shamir and Adleman (RSA) developed an algorithm based on private and public keys which are obtained through generation of random prime numbers in the year 1978 [3]. This algorithm is used as a digital signature by the Reserve Bank of India (RBI) and hacking of the above algorithm is still not recorded in the literature. On the other hand algorithm based on simple XOR, simple mathematical reversible functions like e^x, $\log_e x$ and many more have already been cracked down by the hackers and hacking by intruders have been recorded in the literature. The transacted information in the form of text, audio, video and other kinds of documents may be encrypted into the cipher text and further strong reversible mathematical function must be applied for conversion of cipher text into the plain text as represented in the following figure 3.

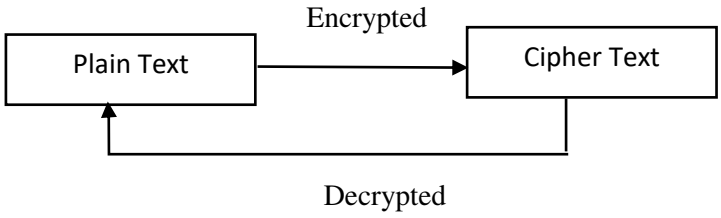

Figure 3Encryption and Decryption of Plain Text

Further, researchers also used ElGamalalgorithm based on the symmetric and asymmetric key encryption and decryption [4] and still cracking of this algorithm is still not recorded in the literature. As described in the figure 1, users are interconnected through various hand-held devices which may be laptop, mobile,

ipad, smart watches and architecture of these devices are already an extension of configuration described by Hwang [5]in the year 1993. Whenever surf over the internet, then there are various kinds of security apps which can protect the data, for example firebase app protects the appIDSeal, Safe Security, Bouncer, Jumbo, F-Secure, Avast mobile security, etc. are the apps which can protect the data available over the hand-held devices. These apps are developed by the scientists and engineers with the help of concepts available in the [6-7].

In the present work, elementary security features are described and there are numerous methods which are applied at various levels of security of data transaction in the form of text, audio and video filed over the internet. Since cyber-crime is occurring in the form of stealing information, hacking of web, stealing of e-mail, and many more which have been described in the Information Technology Act 2000, amended in the year 2018 [18], therefore, the concepts given in the present paper shall minimize the cyber-crime as the data of cyber-crime is increasing daily in India. In the year 2017, 21756 cyber-crime cases were reported which have been increased as 15.3% in the year 2022. Although it is lesser rate in comparison of China i.e., 34% in the year 2022 but it is giving risk signal in India to increase the rate in the subsequent years as technology is moving much more faster than the thinking of individual user. In general, one can say that the developed countries have more rate of cyber-crimes in comparison of the developing countries around the globe.

3. Important Security Features

When the user is well connected through online for accessing the various kinds of website through the hand-held device i.e. considered here as mobile device, then the user has to follow the following suggested measures:

3.1 Hacking of Device

Firstly, user has to know whether the device is hacked by the intruders/hackers. The identity theft and hacking of the device are well covered under the civil and criminal offenses and in India, **Section 66**of the Information Technology Act shall be applicable to the intruders/hackers. But for safety purpose, user can dial the code through the keypad of the mobile device as *≠21≠ which will provide the information that the text, documents, voice are forwarded or not. Accessing of the individual device without consent of the user and illegal collection of data and other documents which are available inside the device; is just simple criminal violation However, if the device is hacked by the intruders/hackers, then for the safety purpose, the user can further dial the code *≠61≠ through which the forwarded text, documents, voice status can be removed. The above codes have been designed by the engineers through the object-oriented computer programming language. When, the above codes have been executed over the mobile device, then, the generated result is shown below in the following figure 4.

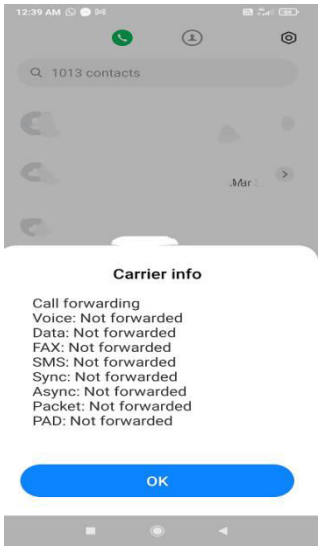

Figure 4.Representation of Mobile Window after Dialling Code *≠61≠

3.2 Hacking of One Time Password (OTP)

Over the network, intruders/hackers are unseen by the users and even user cannot judge about the identity of the hackers/intruders. This situation can be seen when one is getting synchronized text over the mobile device in the form of One Time Password which is a combinations of the numerals and device is synchronized through the Google identity, then the intruders/hackers may easily track the information about the OTP through the Google cloud by running the software codes. Another situation arises, when the PIN is set by the authorised user over the Automated Teller Machine (ATM) and used by unauthorised user over the network for transaction of the digital currency into another account after remembering the card number and pin. This happens when one is getting the information of card of another i.e. relationship of father and son. Unauthorized use of the information of card is covering as cyber-crime covered under the Information Technology Act 2000. In India, when one is visiting to the ATM, only OTP is required for the transaction, and the same is happening when one is transacting the digital currency from one device to another device. Now, to overcome from this situation, Government is moving towards introduction of the concepts of the Artificial Intelligence and Machine Learning. In India, user has identity in the form of Aadhar card in which biometric information about the authorised user is stored, when one is transacting the information in the form of digital currency, then, in place of OTP, in future, user has to verify his thump impression for the biometric authentication. By the use of this concept, only authorised user can transact the e-cash, and it also save the authorised users from the intruders/hackers. Further, geo location of the user can also be added at the time of transaction. The development of research in the field of Artificial Intelligence and Machine Learning will provide a more authentic platform to the users for secure transmission of the e-cash.

3.3 Hacking of Important Information

The information available inside the mobile device is in the form of text, audio and video files and each file may be easily converted into the binary bits supported by the computer system and each bit can be decoded through the security keys which can save from the intruders/hackers. The security keys are based upon the generation of the random numbers. In the old days these keys are based upon the symmetric concept which means that the sender and receiver has similar key which can be used for exchange of confidential information it was just like a lock has two similar keys, later on the idea has been changed and researchers proposed that the keys must be different and it is called asymmetric secure key generation in which send has one key and receiver has different key. The security algorithms are based on

these concepts but hackers/intruders have recorded cracking of the many of the security algorithms developed by the scientists and engineers from time to time.
But for further security of the information of the user's device available in the form of text audio and video, the data is transmitted in the form of chunks and one chunk has one security key, another chunk has another different key and so on. This is known as hybrid cryptography of the information in which multiple security algorithms may be used for strong security of the information. The performance of the hybrid algorithm is much better than the normal security algorithm as depicted in the following table 1.

Table 1 Performance of Hybrid Security Algorithm

Security Algorithm	**Encryption Time in Millisecond**				**Decryption Time in Millisecond**			
File Size→	8KB	16KB	32KB	64KB	8KB	16KB	32KB	64KB
ECC [9]	70	77	79	81	24	20	24	25
Elgamal[9]	12	14	23	45	6	9	11	22
Hybrid	5	10	15	20	2	5	9	18

In the above table, ECC is known as elliptic Curve algorithm, while Elgamal was the scientist who proposed security algorithm. The hybrid cryptography is a combination of the Genetic algorithm along with symmetric key generation. For making the chunks of the information, various kinds of well-known security algorithms may be applied as RSA, ECC, Advanced Encryption Scheme (AES),Secure Hash Standard (SHS) and many more combination of algorithms reported in the literature from time to time.

4. Conclusions

From the above work, it is concluded that users who are attached with hand-held devices well connected over the clouds, must take care at every time when surfing the various websites. It is also suggested that users must change the password in a month time which is used over the different websites, never set the same password on different websites, never share the OTP with anyone which is received over the hand-held device, never click over the phishing web pages, web links and various extension of file format. It is also recommended that the hand-held devices are much rich now to use the Artificial Intelligence services in the form of biometric authentication and hybrid authentications are available over the hand-held devices, therefore, users must use the biometric authentication when visiting the various web pages through the hand-held devices.

5. References

1. *Rivest, R., Shamir,A. and Adleman,L.,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 (2):12-126, (1978).*
2. *ElGamal,T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory,31(4),469-472,(1985).*
3. *Hwang, K., "Advanced Computer Architecture: Parallelism, Scalability, Programmability", Tata McGraw Hill Publication, (1993).*
4. *Blaha, M. and Rumbaugh, J.,"Object-Oriented Modeling and Design with UML", New Jersey, (2005).*
5. *Sarode, S.N. and Chillarge, G.R., "Efficient and Secure Multi-Keyword Ranked Search and Group Data Sharing for Encrypted Cloud Data", Journal of Scientific Research, Vol. 66, No.2, pp. 69-78, (2022).*

Rishi Shukla received his BBA-LL.B degree from Babasaheb Bhimrao Ambedkar University, Lucknow, India and Master of Law from Shri. Ram Swaroop Memorial University, Lucknow, India with Gold Medal. Presently, he is a research scholar in Department of Law, Dr. Ram Manohar Lohia National Law University, Lucknow, India. His research interests are Cyber Crime against Woman, Criminal Law, Deep Learning and Artificial Intelligence.

Dr. Prem Kumar Gautam received his Ph.D. degree from Babasaheb Bhimrao Ambedkar University, Lucknow, India in the field of Human Rights and Constitutional Law. He has 13 years of teaching experience in Criminal Law and published 18 research papers and His research interests are Medicinal & Health Law, Cyber Law and Policy, India and International Criminal Justice.

Manjusha Tiwari received her BA-LL.B and Master of Law degrees from Dr. Ram Manohar Lohia National Law University, Lucknow, India. She has published significant research papers in the field of Environmental and Human Rights, also awarded a best research paper in the 7th National Student Conference, Nirma University, Ahmadabad and presently, she is a research scholar in Department of Law, Dr. Ram Manohar Lohia National Law University, Lucknow, India. Her research interests are Criminal Law, Constitutional Law and Cyber Crime.

Hemant Kumar received MCA degree from Subharti University in the year 2018 and present is a research scholar in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow. His research interest are Software Engineering and Cyber Security.

Prof. Vipin Saxena received his Ph.D. degree from Indian Institute of Technology, Roorkee, Uttarakhand, India. Presently, he is working as Professor in Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India. He has 27 Years of Teaching and 30 Years of Research experience and published more than 200 research articles in the International and National Journals and Conferences, authored 05 books in the field of Computer Science and Scientific Computing, attended 58 International and National Conferences and received three National Awards for meritorious research work in the field of Computer Science.

Corresponding E-mail:[1]***rishi.shukla1504@gmail.com***,*[2]***gautam40.rmlnlu@gmail.com,***
[3]***manjusha902@gmail.com,*** [4]***hemant20192@gmail.com***, [5]***profvipinsaxena@gmail.com***