International Journal of Intelligent Computing and Technology
ISSN: 2457-0249 (Online)
IJICT

Website: https://www.ijict.com June (2019) - Vol.3, Iss.1 Pages:07-13

Remote Biometrics Verification as a remedy to child abuse in Cyberspace using IOT & Onion Routing

[1]Shridhar Hegde, [2]Swati Hedge

[1]Department of Computer Science & Engineering, Ramaiah University of Applied Sciences, Bengaluru, India, [2]Department of Electrical & Electronics Engineering, Vidya Vikas Institute of Engineering and Technology, Mysuru, India

Article History- Received: May 2019; Published: June 2019

Abstract

Over 25 percent of adolescents and teens have been bullied repeatedly through their cell phones or the Internet [1]. Over 14 percent of teenage students have considered suicide, and almost 7 percent have attempted it [2]. This is a problem caused by technological advancement and now only technology can solve it. One cannot find any technical methodologies to solve this problem except a bunch of parental control applications. One can argue that biometric verification can be used to verify the identity but it suffers a huge architectural and security drawback as there are no standard protocols for this specific purpose. Local biometric verification cannot solve this problem. Remote biometric verification used in huge projects like Aadhar and KYC for different banking applications are vulnerable [3]. This paper is about making remote biometric verification more secure and nearly impossible to breach by using principles of IOT and Onion Routing. Complete anonymity is maintained during biometric verification which is ensured by the Onion Routing [4] and the biometric data needed for verification is captured by the IOT devices. This approach can not only be used to solve cyber bullying of children but also many similar problems.

Keywords: —biometric verification, local biometric verification, remote biometric verification, IOT, onion routing, cyber bullying

1. INTRODUCTION

The history of biometric verification dates back to 1858 when Sir William Herschel working for the Civil Service of India, recorded a handprint [5] on the back of a contract for each worker to distinguish employees from others who might claim to be employees when payday arrived. This was the first recorded systematic capture of hand and finger images that were uniformly taken for identification purposes. Now, the institutions that use biometric verification vary from offices, industries and schools to governments & its subsidiaries, intelligence agencies et cetera. At the time of writing this paper, Aadhar is the largest biometric database in the world [5] which is an ambitious project undertaken by Government of India and UIDAI to provide unique identification to the citizens of India. Child abuse has become a major issue [1] in cyberspace and needs to be eliminated or at least minimized by using technology. There are currently no standardized methods, protocols or tools to do this. Works related to the current paper include [6], [12], [13] & [14] which are not totally in the domain of the current paper but relates to it. Biometric verification to prevent online abuse hasn't been provided as the solution. To achieve this, remote biometric verification has to be used which is used for KYC purposes by banks and mobile wallets. It has been found that there is a major flaw in this process by researchers and the database is prone to hack attacks [7].

This establishes a profound need for a robust method which can prevent child abuse online. This paper aims to provide such a robust method using the existing tools, protocols and methodologies which are totally unrelated but has great application when put together. In the current paper, Remote Biometric Verification will be carried out to prevent children from accessing abusive content (which are already flagged as abusive by using AI) in a way that the biometric data is not compromised and the process also remains anonymous.

2. SERIOUSNESS OF CHILD ABUSE IN CYBERSPACE

Cyber Bullying or child abuse on the internet affects day-to-day lives and is a persistent source of distress, worry, depression and the urge to commit suicide. Suicide is the third leading cause of death among young people. Over 14 percent of high school students have considered suicide, and almost 7 percent have attempted it [8]. Bully victims are between 2 to 9 times more likely to consider suicide than non-victims, according to studies by Yale University [11]. According to National Society for the Prevention of Cruelty to Children (NSPCC), 1 in 4 of 8-11 year olds and 3 in 4 of 12-15 olds have a social media profile [10]. In the same report, NSPCC states that 1 in 4 children have experienced something upsetting on a social networking site and around 1 in 8 young people have been bullied on social media. In 2016, the Internet Watch Foundation (IWF) identified over 57,000 URLs containing child sexual abuse images [9]. So, with such content being out there on the internet, the safety of children cannot be ensured and thus the matter has to be considered seriously. This paper aims to provide technological solution to cater safe internet.

3. OVERVIEW OF THE TECHNOLOGIES USED

Remote Biometric Verification/Authentication technology

The related works in the field of Remote Biometric Verification/Authentication systems are [12], [13] and [14]. All the three papers provide mechanisms to enable remote biometric authentication in a secure way using smart cards, secure sketches & fuzzy extractors and one-way hash functions. In order to choose which method will be for remote biometric verification in the proposed system, alternatives have to be discussed and efficient one has to be chosen. In 1981, Lamport [15] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. In Lamport's scheme, password table was used to verify the legitimacy of users but if this password table is compromised, stolen, or modified by an adversary, then the system could be partially or completely compromised [14]. So, this method cannot be used. After reviewing some other works related to Remote Identity Verification, Khan-Zhang's scheme [14] for remote biometric verification can be declared as the efficient method to be used. In future, if this idea is to be implemented, any other authentication methods standardized during the time can be used.

Capturing biometric data using IOT

Internet of Things (IOT) is a booming branch in the field of technology. The concepts of this branch can be used where all the devices are connected to the internet and can communicate to each other. In order to obtain the data required for the biometric verification, the first device to look out for will be the smartphones. The recent day smartphones have local fingerprint recognition on them and this module can be used to obtain data required for the remote biometric authentication. For devices which do not have an inbuilt fingerprint module, CrucialTec's standalone fingerprint scanner for IOT devices [17] can be used. This device is special as it has its own embedded processor and does not need help from any external processor chips. This makes it a typical IOT device to be used in the current system being built. This device fits into every electronic device we use such as PC, TV, refrigerator et cetera as the prior is only 17 mm2 in dimension consuming 30 mAh.

Onion Routing

Onion Routing [18] is a general-purpose infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. The connections are bidirectional and nearly real-time. In a typical client-server communication over a public network such as internet, the client which requires a service sends a service request message to the server which is located in a remote place. The service request message is routed to the server from the client's machine through the ISP (Internet Service Provider) and many other nodes on the way. This means that the identity of the client is open in the air. In order to prevent this, Onion Routing was introduced. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion. The encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. When the final

layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes [18].

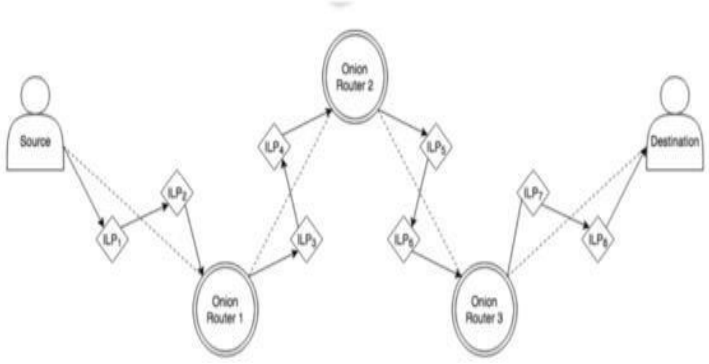

Fig 1: Onion Routing on ILP (InerLedger Protocol) [20]

Figure 1 shows a three-layered onion routing system. The three layers are named as entry guard node, middle relay node and exit relay node. The three nodes have different encryption keys and do not know the service request message as it is encrypted. Only the client knows the original message sent and all the three keys.

4. PROPOSED SYSTEM

In this section, a solution will be formulated to solve the problem of child abuse in cyberspace using technologies described in III.A, III.B and III.C. Remote Biometric Verification / Authentication, capturing fingerprints through IOT and Onion Routing are totally unrelated technologies which are not a good fit together but in the current system proposed, they will blend in to solve the problem at hand.

Assumptions made before defining the proposed system

Before diving into the description of the system, the term "red flagged content" has to be understood in the current context. The government has to build a system which identifies potentially harmful content for children using AI (Artificial Intelligence). The red flagged refers to websites, applications/software or anything on the internet that can be termed as inappropriate or harmful to children (a separate research paper can be written on the process of classifying content as red flagged or not). Any more explanations about red flagged content would be out of the scope of this paper. To verify the biometric data, the government must build servers that are placed in multiple parts of the country. These servers are exactly the same as Aadhar database but only the fingerprint data and the age of the person is stored with strong encryption. Even if the servers are compromised, personal data of the clients are not exposed. The people in possession of compromised fingerprint and age of a person cannot do anything with the data unless the identity of the person whose data is in possession is known. This method is less risky than the Aadhar database which stores every single personal information about the person.

The proposed system

The clients (in this case, children) who are using the internet have to verify their identity whenever a reg flagged content is accessed. Their identity will be verified using the Remote Biometric Verification/Authentication as described in III.A. But the data which is sent and received is encrypted as per the protocols of onion outing. This is discussed in the later part of the paper.

The identity of clients are verified against their fingerprint database. The clients (children) have to provide their fingerprint data which is captured either through their smartphone's fingerprint module (if there is one) or devices like the IOT standalone fingerprint module described in III.B.

Finally, the fingerprint data is encrypted with three different keys and the request is made though onion routing phenomenon (visualization can be seen in [19]) which will ensure safety and anonymity of the user and makes the system less vulnerable. Although, "timing analysis" can be used to decode the information and compromise the system. If the verification servers set up by the government are included inside the Tor Hidden Services, then there is no way the identity of the client can be identified or the data can be compromised.

5. ADVANTAGES AND DRAWBACKS OF THE PROPOSED SOLUTION

A. Advantages The proposed system provides a solution to child abuse on the internet by using existing technologies. The main advantage of the proposed system is that it is secure due to various standardized protocols that are involved. The system also preserves the anonymity of the client. In case of data breaches in the central database maintained by the government to implement the proposed system, the compromised data wouldn't pose practical threat because only fingerprint data and age of a person are compromised. This will be of no practical use as the person's private information are not bound to the compromised data. Also, if the central database is made as part of the Tor Hidden Services, then there is no way of data being compromised as no eavesdropper would know the identity of the server. B. Drawbacks The apparent drawback about the proposed system at the time of writing the paper is that it is costly to implement. The initial investment on the project is so high that it has to be undertaken only by the government or companies that have proper resources. The proposed system when implemented for practical applications might be slower in execution as there are various protocols of three different technologies underlying in the system.

VI. CONCLUSION

The current paper gives insight only about the high-level implementation of the system and welcomes more research and validation on the same. The authors are yet to design fully working and practical mathematical model for the proposed system. After thorough analysis of the designed high-level model, it can be concluded that the proposed system can give a remedy to the abuse of children in cyberspace. The system not only solves the child abuse

online problem but also has many other practical uses which if needed can be modified accordingly.

ACKNOWLEDGEMENT

The authors would like to thank authors of all the cited works who have made the research easy and feasible. A huge thanks also goes to the pioneer designers of Remote Biometric Authentication, IOT Biometric data capturing devices and Onion Routing.

REFERENCES

1. Cyberbullying Research Center, Summary of our cyberbullying research from 2004-2010 (online). Available at: https://cyberbullying.org/summary-of-our-cyberbullying-research [Accessed 23 Mar. 2019]
2. The Organic Academy, The Life and Death Consequences of Cyber Bullying (online). Availabel at: https://theorganicagency.com/blog/life-death-consequences-cyberbullying/ [Accessed 23 Mar. 2019]
3. The Economic Times, Indane leaked millions of Aadhar numbers: French security researcher (online)
4. Hooks, Matt & Miles, Jadrian & Reynolds, Patrick & Astrachan, Owen (2006), Onion routing and online anonymity
5. The History of Fingerprints (online). Available at: http://onin.com/fp/fphistory.html [Accesed 25 Mar. 2019].
6. Takahashi (2018), "Authenteq launches blockchain identity verification to stop online trolls",Media Report. Available at : https://venturebeat.com/2018/08/30/authenteq-launches-blockchainidentity-verification-to-stop-online-trolls/ [Accessed 26 Mar. 2019].
7. Khaira, Rachana, Sethi, Aman, Sathe and Gopal (2018), UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm (online). Available at: https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-softwarehacked-id-database-compromised-experts-confirm_a_23522472/ [Accessed 26 Mar. 2019].
8. Kim YS, Leventhal B (2008), Bullying and suicide- A review, International Journal of Adolescent Medicine and Health, 20(2), pp.133–154
9. IWF Annual Report (2016) Available at: https://www.iwf.org.uk/sites/default/files/ reports/ 201704/iwf_report_2016.pdf [Accessed 28 Mar. 2019].
10. Holly Bentley et all. (2018), How safe are our children? Availabe at: https://learning.nspcc.org.uk/media/1067/how-safe-are-our-children2018.pdf
11. Yale University (2008), Bullying-suicide link explored in new study by researchers at Yale (online). Available at: https://news.yale.edu/2008/07/16/bullying-suicide-link-explored-newstudy-researchers-yale
12. Li, Chun-Ta., Hwang, Min-Shiang. (2010), An efficient biometricsbased remote user authentication scheme using smart cards, , Journal of Network and Computer Applications, 33(1), pp.1-5 [doi>10.1016/j.jnca.2009.08.001]
13. Boyen, Xavier., Dodis, Yevgeniy., Katz, Jonathan., Ostrovsky, Rafail., Smith, Adam., Cramer, Ronald (2005), Secure Remote Authentication Using Biometric Data, Proceeding

EUROCRYPT'05 Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, ISBN:3-540-25910-4 978-3-540-25910-7Pages 147-163

14. Khan, M. and Zhang, J. (2007), Improving the security of 'a flexible biometrics remote user authentication scheme', Computer Standards & Interfaces 29(1), pp.82–85
15. L. Lamport (1981), Password authentication with insecure communication, Communication of the ACM, 24(11), pp. 770-772.
16. M. S. Hwang and L. H. Li (2000), A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, 46(1), pp. 28-30
17. CrucialTec develops fingerprint scanner for IoT devices (online). Available at: http://www.theinvestor.co.kr/view.php?ud=20170331000614 [Accessed 30 Mar. 2019].
18. Goldschlag D, Reed M and Syverson P, (1999), Onion Routing for Anonymous and Private Internet Connections, Communications of the ACM, 42(2)
19. AlQahtani, Abdullah & El-Alfy, El-Sayed (2015), Anonymous Connections Based on Onion Routing: A Review and a Visualization Tool, Procedia Computer Science. 52. 10.1016/j.procs.2015.05.040.
20. Khosla, Akash., Saran, Vedant, Zoghb and Nick. (2018), Techniques for Privacy Over the Interledger, University of California

How to cite this article:
Shridhar Hegde & Swati Hedge, "Remote Biometrics Verification as a remedy to child abuse in Cyberspace using IOT & Onion Routing", International Journal of Intelligent Computing and Technology (IJICT), Vol.3, Iss.1, pp.07-13, 2019