Mitigating Cyber-Threat in the Financial Industry of Bangladesh using Biometric based Public Key Infrastructure (PKI) with the Help of Digital Certification

Rifat Tasnim Anannya[1] and Sifat Rahman Ahona[2]
[1]Lecturer, Department of Computer Science, American International University, BANGLADESH
[2]Lecturer, Department of Computer Science, American International University BANGLADESH

[1]Corresponding Author: rifat.tasnim@aiub.edu

ABSTRACT

Information is such a thing which if misused, leaked or breached can lead to undesirable consequences. Financial institutions have a lot of data of their customers. These data's are regarding customers' personal information, transactions and many more which are highly sensitive. The entire system by which financial institutions such as – banks run, are required to be secured from cyber breach. As by breaching these systems' can lead to financial disaster. The rapid growth of IT infrastructure is not only considered a convenient way for customers in many perspectives but also it point out the lack of skilled manpower in our country. In banking sector, ATM, E-money laundering are the domain where crime occurred most of the time. So, this paper focuses on developing a conceptual framework based on secondary sources which included publications, journal, books etc. regarding the problem of cyber-threat happening in Bangladesh. It describes how a financial institute can make safe transaction using biometric based public key infrastructure with the help of digital certificate.

***Keywords*—** Biometric, Cyber Security, Cyber Crime, Digital Signature, Electronic Fund Transfer, Public Key Infrastructure

I. INTRODUCTION

In Bangladesh banking is one of the most prominent business sectors. The biggest challenge for banks is to protect the large no of customer information & transaction records. Now-a-days banking service has spread in such a way that customer can make a transaction from wherever they want via (electronic and other alternative delivery channel). Through electronic service millions of people send remittance from abroad. So, it is important for banking industry to update their infrastructure for the sake of information security because information is one of the most vital resources for a bank. To provide better electronic services, adoption of information technology is a necessity now.

Banking industry contributes a significant portion to the economy. In Bangladesh all the private banks tried to follow information technology from their starting. So that, they can always fulfill their customers' expectation. It creates a strong business bonding among customers & banks. As the growth of information technology is improving faster, if we put the technological knowledge in a proper place we can make our electronic banking system smoother & more secured. Though Bangladesh is a comparatively low adoptee in terms of information technology but now every bank should try to follow the technological policy for the betterment of customers & their own, but sometimes the use of technology leads us to the destructive activities which is known as cyber-crime. Innovation, profit, growth all the positive sides of banking is happening because of the electronic fund transfer (EFT). It includes ATM, POS,e-banking since 2001. [1] By adopting these technologies banks are able to tie the customer closer to them. On the other hand this dependency has increased the risk for customers because the current condition of cybercrime occurring in Bangladesh from last few years is quite high. So, it is high time to reducing the lack of security in IT sector. Accuracy, appropriateness, correctness, timely delivery are only possible from the bank end when they have an updated technological infrastructure which is supported by IT.

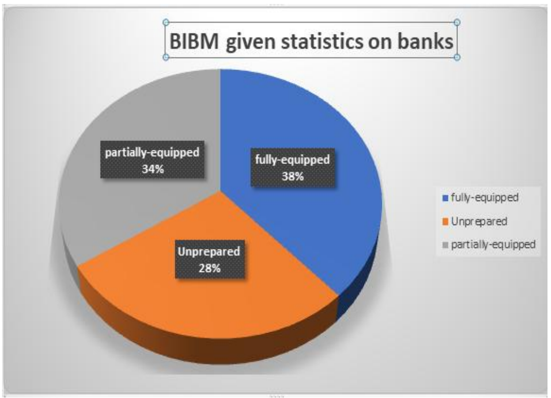

Figure 1: BIBM given statistics on banks

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.1

Recent Cyber Security Threats in Banking

Financial institutions are facing digital threats in a regular manner now a days. Cybercrime groups have used modern techniques. It has been also noted that because of the immature security systems, young financial technological companies and crypto-exchanges are most vulnerable. In 2018 AppleJeus attacked the cryptocurrency traders which is most innovative in our opinion. At that instant, special software which seemed lawful was created. Nonetheless, a malicious update has been uploaded stealthily. Some common kind of threats of past years are given below:

Ransomware & Malware

In every 14 seconds someone might become a victim of cyber attack as Ransomware has already damaged $11.5B already in the year 2019. It becomes more costly than traditional data breaches in case of denying access to a computer or system using malware or software until a ransom is paid.

It has commonly been assumed that it damages billions of dollars of the victims every year, as hackers uses technologies which facilitate them to abduct the database of any organization and occupy all of the information for ransom. [13]

Endpoint Attacks

As companies are using cloud more and more to store resources, the size of the attack surfaces will continue to grow. Because of the bring-your-own-device culture combined with the growth of SaaS providers for data services, angles of hacking has been increased. [14][19]

Phishing

It is widely known that phishing is one of the economical and effortless ways to compromise the target. Mostly, delivering malware to ones device by using regular emails from trusted sources and giving opportunity to the hacker the access they wish. With the expansion of SaaS services like Dropbox, Office 365, Salesforce and others, hackers are boosting up their skills with more disenchanted attack types. [14]

Third Party & Supply Chain Attacks

A supply chain attack (also called a third-party attack) occurs when ones system gets penetrated through an outsider who has access to ones systems. Because of the expansion of digital supply chains, hackers have immense opportunities, and incursion of this sort are becoming more apparent. When working with third parties, Security patches and software updates are critical protections and another area of vulnerability. For updates and patches most third-party software is dependent on resources and foreign libraries. System updates is being redirected to malicious servers to deliver malware to their victims, if these external resources are compromised. [15]

State-Sponsored Attacks

By stealing individual and corporate data now a days entire nation states are now using their cyber techniques to permeate other governments and they are also performing attacks on critical infrastructure. Now a day's cybercrime is not limited to private sector but also expanded in the bureaucratic sector. [16]

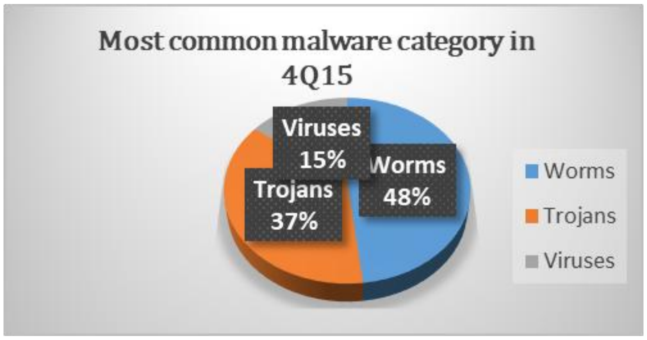

Figure 2: Most common malware attack [6]

II. BACKGROUND STUDY

In last few years banking industry faced several security breaches which is alarming for our country.

On January 06, 2013, Islami Bank Bangladesh site was hacked by Human Mind Cracker.[7] In 2013, Sonali Bank of Bangladesh was also effectively targeted by hackers who were successfully take away $0.25 million.[7]

ATM card fraud happened in February 2016 when skimming devices were implanted in several ATM booths of some banks to snip card information and create duplicates, according to Bangladesh Bank the country witnessed its biggest fraud.[4] Nearly Tk 10 million was deceived which affected City Bank, EBL, United Commercial Bank and Premier Bank.[4] City Bank was forced to repay a substantial amount to its customers whose cards were deceived. Brac Bank also repaid Tk 0.7 million to its customers for the same cause in April, 2018.[4]

On February 4, 2016, anonymous hackers stole a total of $101 million from Bangladesh Bank's account at the Federal Reserve Bank of New York, using false orders on the SWIFT payments system.[10] Immediately $20 million was shifted to Sri Lanka which was clogged.
But the $81 million sent to accounts at Manila-based RCBC had vanished into the casino industry in the Philippines. Bangladesh Bank has decided to heading a case against Philippines' Rizal Commercial Banking Corporation (RCBC).[10] On November 10 last year, Philippines had sent back $14 million to Bangladesh Bank resulting a court order, which was recovered mostly from a Manila casino junket operator.[1] After this incident, The government formed the BGD e-Gov CIRT ('cyber incident response team') under the Bangladesh Computer Council (BCC)[5].

CIRT also met hundreds of attacks on the Election Commission Secretariat website throughout the election passé in December last..

Again, On June 1,2019,Dutch Bangla Bank Limited (DBBL) loses as much as $3 million (around Tk 25 crore) to global cybercriminals, according to the banking sector.[3][9]Two other banks -- NCC Bank and Prime Bank -- also faced cyber attacks, but they claimed they were able to prevent financial losses. Using malware or cloning credit or debit card hacker always try to hack customers information. Bank could not detect that around three months ago hackers planted a malware in the bank's switch (card management system) and made a perfect replica of the switch.. When hackers went for transactions last month, the proxy or the shadow switch gave commands to release funds while bank completely in the dark mode. Around a couple of weeks later, the DBBL's nine ATMs fell prey to an international hacker group that took around Tk 16 lakh on May 31. Law enforcers later detained six Ukrainians hackers for this cyber crime.

The above attack clearly shows that there is a huge lacking in the infrastructure of IT in banking industry.

Unqualified human resources were selected without proper evaluation of technical skills. banking sector has left itself wide open to sophisticated hacking operations after all these crime & does not follow the government policy seriously. ! It seems that the sector's senior management has not taken this instruction to heart.

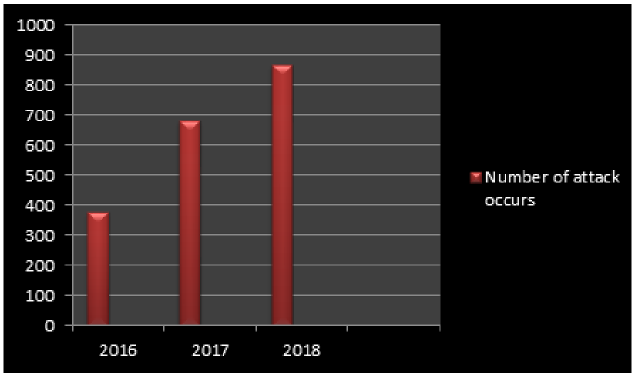

Figure 3: Number of cyber-attacks.

Security Goals

There are many general security principles but the most common three security goals are:
Confidentiality, Integrity and Availability.[17]

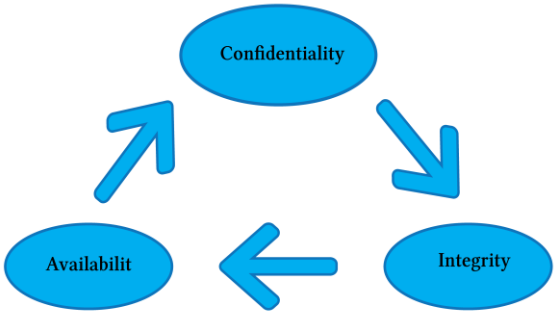

Figure 4: Security goals

Confidentiality

It is also known as secrecy. It is about protecting business data from unauthorized user. It means that information is only being used by people who are authorized to access it. Confidentiality is about controlling access to files either in transit or in storage from unauthorized user. [17]

Integrity

It means assets can be modified or deleted only by authorized people in an authorized way. Thus, the change of information by an unauthorized people is impossible and changes occurred by authorized people are also stored. [17]

Availability

It means assets are continuously available to user in a timely manner. This means the information is available to user when the user needs it. The failure to meet the requirement is called denial of service. [17]

III. METHODOLOGY

To achieve an updated infrastructure in EFT, many techniques such as encryption techniques, anti-skimming devices, authentication mechanisms are used in bank to ensure secure data transmission. This paper first of all introduces some frequently used mechanisms such as biometric, digital signatures using public key infrastructure and after that suggests a new approach named Biometric based Public Key Infrastructure (PKI) with the help of Digital Certification.

Biometric-

In our lives sometimes we face a situation where we need to prove who we are; may it be for personal reasons or as part of your profession or it can be for verification. Biometric is such a technique which proves our identity by following these steps- data capture, enrollment, authentication & matching. Using biometric based systems it is possible to authenticate and identify of an individual by processing their biometric data. Different biometric identifiers are frequently used, one is physiological & another is behavioral. The most common

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.1

biometric identifiers used in authentication system is fingerprint according to the given survey. But also there are lots of others method like iris which is comparatively low equal error rate. [2, 20]

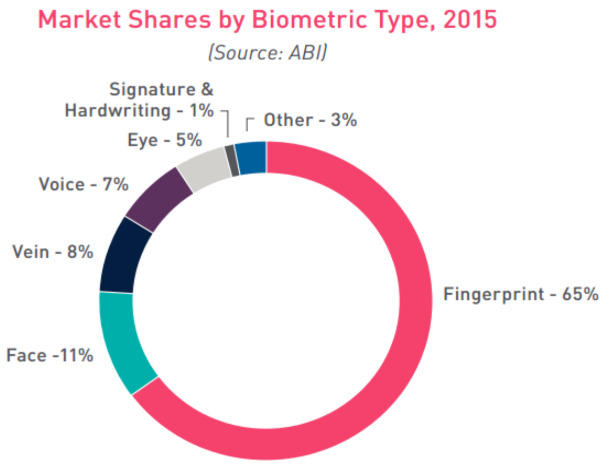

Figure 5: Biometrics market share by system type, based on revenue.

Public Key Cryptosystem

Asymmetric cryptography or Public-key cryptography is an encryption scheme that uses two dissimilar mathematically related keys such as public key and a private key. Unlike symmetric key algorithms this algorithm depends on one key to both encrypt and decrypt. In this method key performs a individual function every time. In order to encrypt public key is used and to decrypt private key is used.

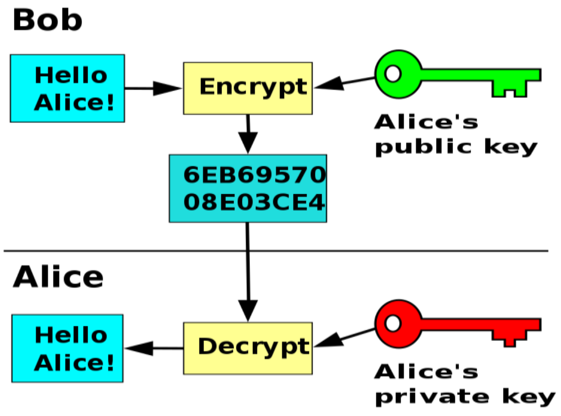

Figure 6: Public key cryptosystem

It is not computationally feasible to compute the private key on the basis of public key. For this reason, public keys can be shared easily and allow users a convenient method for data encryption and verify digital signatures, and private keys are kept secret, as decryption of the content can only be done using private keys and owner can create digital signatures. [12]

Digital Signature

To ensure updated infrastructure in terms of security it is necessary to accomplish the basic security goal during its implementation. Digital signature is a mathematical scheme for validating the legitimacy of digital messages, it also guarantees that the contents of a message have not been altered in transit. Digital signature process includes one hash function & public key cryptosystem. Hash function is a one directional algorithm which created message digest. By encrypting this message digest with the help of sender’s private key, the signature is created. The receiver uses the sender's public key and the same hash function to authenticate the received signature where no confusions are exist.[21]

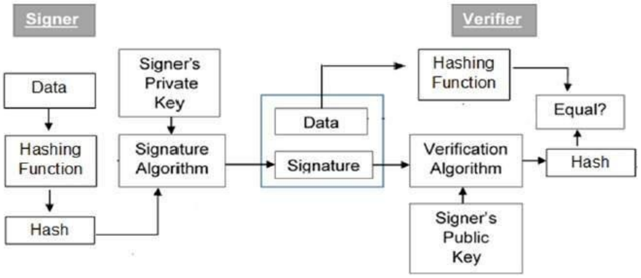

Figure 7: Digital signature [11]

Biometric based Public Key Infrastructure (PKI) with the help of Digital Certification method

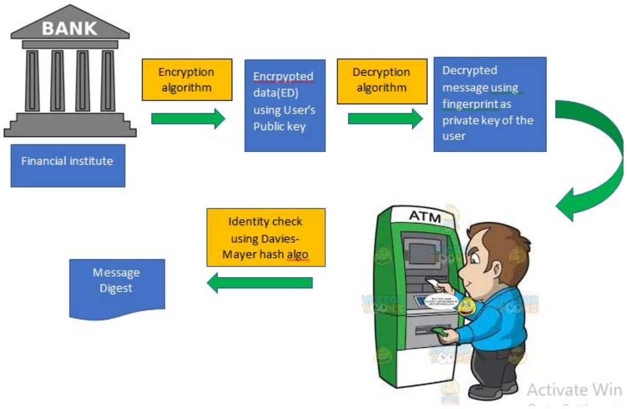
BANK
Financial institute
Encryption algorithm
Encrpypted data(ED) using User's Public key
Decryption algorithm
Decrypted message using fingerprint as private key of the user
ATM
Identity check using Davies-Mayer hash algo
Message Digest
Activate Win

Figure 8: Phase-1 Transaction between bank & user

IV. OUR APPROACH

In our proposed method we are using the most common biometric pattern which is known as fingerprint. Due to our national id registration system the concept of using fingerprint is most suitable for Bangladesh. Also the original grey scale fingerprint image has a bit depth of 8 bits, and depending on sensor size each such an image will require a few Mbytes of storage which require less investment. Another reason of using biometric system is its anti-hacking measure, its mathematical representation is stored as a template in a device. Storing the representation reduces hacking risks & the algorithm which involved in the authentication process are run in a Trusted Execution Environment (TEE)[15]. We are using public key infrastructure in digital signature to provide secure & valid communication between bank & clients. Generally when a bank opens an account for a customer it must keep his/her national id as a proof of identity. During the implementation of phase 1 digital signature NID number is considered as public key for a bank whereas fingerprint is considered as a private key from user's side. Since, we knew that, for national id registration process fingerprint is stored in database where duplicate data is impossible. So, during the transaction from a bank, it must encrypt its info through national id which is a public key in our scenario. According to the policy user should able to decrypt the message using his/her fingerprint which cannot be done by hackers. After retrieving the data the user will check the source identity for which we are using a hash algorithm known as Davies-Meyer. [14] This algorithm works for message-block(mi) & generate different hash values(hi) for each block & xor the message with previous hash value(hi-1).

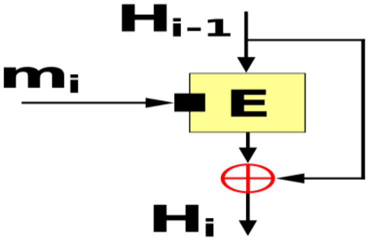

Figure 9: Davies-Meyer algorithm [8]

Using this algorithm, the main message will be converted to message digest. Now if we want to identify that the source is actual or fake or for achieving authentication we can implement the second phase of digital signature.

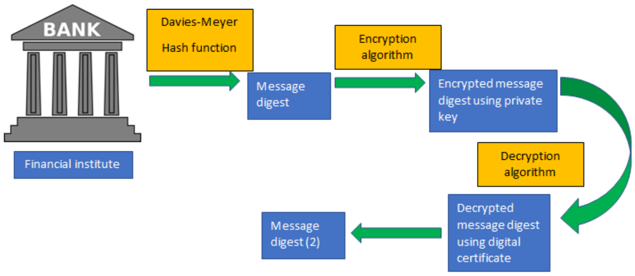

Figure 10: Phase-2 Identity proof & integrity checking

Here first the bank need to convert their data to a digest mode using davies-meyer algorithm. All the data which is stored in the bank should be encrypted & again decrypted using bank's public key. Bank's public key is a certification number which is issued by certificate authority(CA).

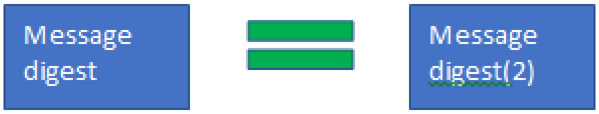

Figure 11: Phase 2.1 Integrity Proof

Then we will get our digested data. If both digested data are matched then integrity can be achieved.

Future Work

Here we are working using davies-meyer algorithm. It is possible to compute fixed points for the construction. For long message the complexity is above 2n/2 but when the messages get shorter the complexity of the attack approaches to 2n. [18] This paper also focuses on financial institute of Bangladesh. Bangladesh has a limited infrastructure facility and limited skill manpower. Information technology is very ignorant and Computer literacy was found very few.

V. CONCLUSION

In this paper we are using the most common biometric pattern which is known as fingerprint. Due to our national id registration system the concept of using fingerprint is most suitable for Bangladesh. The focus of this paper is mainly based on davies-meyer algorithm which is a one way algorithm. This method describes how a financial institute can make safe transaction for mitigating cyber-attack. Cyber-crime is an alarming issue now, which needs to be solved immediately. Recommendation can be given by Bangladesh bank to all the banks to strictly follow our proposed lifecycle for ensuring the updated infrastructure. On the other hand senior management can play an important role to create awareness among customers & management. Ensuring IT governance can be a solution to control this hazard situation.

ACKNOWLEDGMENTS

First of all we express our gratefulness to the Almighty Allah, without His divine blessing it would not be possible for us to complete this research work. We are also grateful to all of our respected teachers without whom we would never at this educational stage. Last but not least we would like to show our gratitude to our parents for being so understanding.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.1

REFERENCES

[1] Mahbub Rahman, Nilanjan Kumar Saha, Md. Nazirul Islam Sarker, Arifin Sultana, & A. Z. M. Shafiullah Prodhan. (2017). Problems and prospects of electronic banking in Bangladesh: A case study on Dutch-Bangla bank limited. *American Journal of Operations Management and Information Systems, 2*(1), 42-53. doi: 10.11648/j.ajomis.20170201.17.

[2] J.A. Unar, Woo Chaw Seng, & Almas Abbasi. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition, 47*(8), 2673-2688.

[3] Sultana Sharmeen Karim. (2016). Cyber-crime scenario in banking sector of Bangladesh: An overview. Available at: https://slidex.tips/download/cyber-crime-scenario-in-banking-sector-of-bangladesh-an-overview.

[4] Cyber-attacks continue to rise in Bangladesh. (2019). Available at: https://thefinancialexpress.com.bd/sci-tech/cyber-attacks-continue-to-rise-in-bangladesh-1549427552.

[5] Joyanta Saha. (2019). Bangladesh turning focus to cyber security, ICT state minister. Available at: https://bdnews24.com/technology/2019/01/25/bangladesh-turning-focus-to-cyber-security-ict-state-minister.

[6] Hackers steal $1.8m from 2 private banks. (2019). Available at: https://www.dhakatribune.com/business/banks/2019/06/22/hackers-steal-1-8m-from-2-private-banks.

[7] Common vulnerabilities in cyber space of Bangladesh. (2019). Available at: https://www.cirt.gov.bd/common-vulnerabilities-in-cyber-space-of-bangladesh/.

[8] One-way function. (2019). Available at: http://www.crypto-it.net/eng/theory/one-way-function.html

[9] Three banks hit by cyber attacks. (2019). Available at: https://www.thedailystar.net/frontpage/news/three-banks-hit-cyberattacks-1760629.

[10] Bangladesh bank ready to sue filipino bank for failing to return $66.46m of heist money. (2018). Available at: https://www.dhakatribune.com/business/banks/2018/02/07/bb-file-case-rcbc-fail-return-heist-money.

[11] Cryptography digital signatures. (2019). Available at: https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm.

[12] Public-key cryptography. (2019). Available at: https://en.wikipedia.org/wiki/Public-key_cryptography.

[13] Ransomware. (2019). Available at: https://en.wikipedia.org/wiki/Ransomware.

[14] Know the types of cyber threats. (2019). Available at: https://www.mass.gov/service-details/know-the-types-of-cyber-threats.

[15] What is a supply chain attack? Why you should be wary of third-party providers. (2019). Available at: https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html.

[16] State-sponsored cyber attacks. (2018). Available at: https://www.mwrinfosecurity.com/our-thinking/state-sponsored-cyber-attacks/.

[17] Pearson IT certification. (2019). Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=3.

[18] One-way function. (2018). Available at: http://www.crypto-it.net/eng/theory/one-way-function.html.

[19] What is endpoint security?. (2019). Available at: https://www.forcepoint.com/cyber-edu/endpoint-security.

[20] Fingerprints biometric technologies whitepaper 2017. (2017). Available at: https://www.fingerprints.com/asset/assets/downloads/fingerprints-biometric-technologies-whitepaper-2017-revb.pdf.

[21] Shafi Goldwasser, Silvio Micali, & Ronald L.Rivest, A digital signature scheme secure against adaptive chosen-massage attacks. (1988 Apr). Available at: https://people.csail.mit.edu/rivest/GoldwasserMicaliRivest-ADigitalSignatureSchemeSecureAgainstAdaptiveChosenMessageAttacks.pdf.