Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management

Ishaq Azhar Mohammed

Sr. Data Scientist & Department of Information Technology

Dubai, UAE

Abstract*-The main purpose of this paper is to explore the concept of identity-based encryption which will focus on identity and access management to enterprise privacy. In today's society, data privacy is a very sensitive subject. Data may be stored or sent, encryption is a strong key component for the anonymity and protection of information [1]. It has two larger ranges: symmetric and asymmetric. Two keys for encrypting and decrypting are needed for asymmetric systems, whereas a single key for encryption and decryption is used in asymmetric systems. Identity-Based Encryption is a kind of asymmetric cryptography that is used to protect sensitive information. To simplify the certificate handling, the message is encrypted by arbitrary strings. The bulk of our communications are carried out online with the aid of amazing technological progress. This is why encryption is more essential than ever before. In today's world, we rely heavily on technological communications. For commercial and communication reasons, we transmit data, movies, images [1]. We communicate through internet services such as social networks and messaging applications. We're sending millions of emails, downloading lots of information. As a consequence, we place ourselves in a position of extreme vulnerability. If they take over our digital communications, hackers, malicious hackers or assailants may damage us. That is why we use a variety of cryptographic techniques to guarantee the security and integrity of our interactions [2]. Identity-Based Encryption is one of the most common types of encryption and provides comprehensive security for people and organizations. This article will examine in depth what identification-based encryption is and why many companies need it for security purposes.*

Keywords: *Identity-based encryption, encryption, decryption, Identity access management, Private Key Generator, Private key, Public key, ciphertext.*

I. INTRODUCTION

In 1984, Shamir first came up with the idea of identity-based encryption (IBE). Originally, he wanted to do away with the requirement for databases and certifications by storing the public key in the recipient's identity instead of in a database. Whilst answers to the associated ID-based signature issue have been discovered rapidly, identity-based encryption has been harder. The primary objective of Identity-based encryptions functionality is to streamline the administration of certificates and thus remove the need for certifying authorities (CA) [2]. In general, a public-key certificate in Public Key Infrastructure (PKI) is necessary to tie the signature to the identity of a person. However, certificates are unnecessary with identity-based encryption, because every user is tightly bound by his/her identification. Encryption based on identity needs a Private Key Generator (PKG) for the creation and delivery to registered members of the private key. In 2001 Boneh and Franklin developed the first viable and provenly secure IBE method utilizing bilinear combinations in elliptical curve groups. The same year, Cocks created an IBE plan based on the issue of quadratic residuosity, although it was very inefficient. Boneh, Gentry, and Hamburg subsequently developed a more efficient, provenly safe method based on the same issue [2]. This paper is aimed at presenting the findings and providing a critical assessment of how IBE was used to offer all the well-known cybersecurity services for companies.

II. PROBLEM STATEMENT

The main problem that this paper will try to solve is to understand how identity-based encryption offers more protection to enterprises from identity and access management to enterprise privacy. Here, the major issue is how identity-based encryption provides companies with more security against identity and access management to business confidentiality. Public-key encryption provides extremely robust electronic communications security [3]. Much of their power lies in using paired keys that are distinct codes that encrypt and decode a communication but are mathematically linked. One key is open and one is known to the receiver alone. But nobody uses cryptography with a public key, since that's too much hassle. The receiver must be equipped with private and public keys, and the recipient must be able to know or discover the public key of the recipient. This implies in most instances that the sender needs an authentication mechanism to get the public key of the destination recipient [3]. Although this is easy in a business, senders outside of the organization have no access to a centralized directory, thus sending encrypted communications is more complicated for them. In addition, the procedure only works when the receiver decides to utilize it and possesses a key. And the majority of individuals have no public keys. A potential solution to these problems is termed identity-based encryption (IBE). A unique identity of the receiver (e.g. his email address) may be utilized to generate a public key in this procedure, which can be started by the sender. To generate the matching private key from a public key, a trustworthy third-party server, termed the private key generator, employs a cryptographical algorithm [3,4]. Thus, receivers may immediately create their private keys from the server when necessary and don't have to concern about sharing their public keys.

III. LITERATURE REVIEW

A. Encryption

Encryption is a way of converting information into a digital signature that conceals the actual interpretation of the information. Cryptography is the science of encryption and decryption. In the computer process, unencrypted data is sometimes referred to as plaintext while encrypted data is referred to as ciphertext. The formula for encoding and decoding communications is termed encryption algorithms or ciphers [4]. To be successful, a cipher's algorithm must contain a variable. The variable, referred to as a key, is what

distinguishes the output of a cipher. Whenever an unauthorized party intercepts an encrypted communication, the intruder must figure out the sender's cipher to encrypted in the message, and the key variables to be utilized. The time and complexity of conjecture are what making encrypting such a useful security device. Encryption has long been a popular method of safeguarding sensitive data [4,5]. The military and governments have historically utilized it. Modern encryption protects data saved on computers, storage systems, and transmits data across networks.

B. Encryption key management and wrapping

Encryption is an excellent method of data security, but the cryptographic keys must be maintained properly to guarantee that data stays secure while being accessible when required. Encryption key access should be controlled and restricted to those who must use it [6]. An audit should be conducted to provide a baseline for how the company configures, monitors examine and manages access to encryption keys. Key management software may also assist centralize key management and secure keys against illegal access, replacement, or alteration [6,7]. Key wrapping is a kind of security feature available in certain key software management systems that effectively secures the encryption keys of a company individually or in large numbers. The process of decryption of wrapped keys is termed unwrapping. Typically, key wrapping and unwrapping operations are performed using symmetric encryption [8].

C. Encryption based on identity

Identity-based encryption (IBE) is a public key encryption method where a third-party server utilizes a basic identifier such as an email address to create a public key to encrypt and decode electronic communications. Every string is considered an appropriate public key in this environment. In other words, information like e-mail addresses or dates may be public keys [8]. If the email sender gets accessibility to a system's public parameters, they may encrypt the message with a text value, such as the email address of the recipient. Compared to traditional public-key cryptography, this significantly lowers the sophistication of both users' and administrators' encryption processes. An additional benefit is that a message receiver doesn't require prior preparation or specialist software to interpret the message [9]. IBE makes cryptography easier to understand for text admins, senders, and recipients. Identity-based encryption is generally seen as an important primordial form of ID-based encryption. Furthermore, it is considered to be a sub-type of public-key encryption. Adi Shamir invented ID-based encryption in the 1980s [9]. He initially proposed identity-based signatures as a form of encryption but he was not able to contribute positively to the identity-based encryption issue. However, it wasn't until 2001 when a novel combination of the Boneh-Franklin method and Cocks' encryption algorithm was able to solve the problems presented by identity-based encryption [9,10].

D. How IBE Works

Identity-based encryption offers an easy operating concept. It enables both the sender and the recipient to create a public key from a text value based on an established identity. The success of IBE relies on the IBE server from a third party that produces private keys [11]. This third party is also known as the Private Key Generator, and it generates private keys as its name implies.

First and foremost, the Private Key Generator creates a master publish key and stores a matching master private key in its database (also known as the master key). The only content permanently stored by this server is a secret master key - a big random number exclusively for the security field [12]. This key is used by the servers to generate a shared set of public important components (including the server address) for each user who installs IBE software as well as the private key of the receivers as needed.

Senders and recipients may then calculate a public key that matches the identity by combining identity and master key. The authorized person has to access the Private Key Generator to get the appropriate private key [13]. Whenever a sender produces an encrypted message, IBE on the system utilizes three variables to construct the public key: a starting value, the present week number as well as the identity of the sender which can normally involve an e-mail address. Since a calendar reference is provided, the created public key immediately expires [13]. A user who gets an IBE-encoded e-mail but it has not used the procedure previously may obtain a private key to decode all e-mails encrypted using their e-mail address as a public key, following authentication. This method enables entities to encrypt their communications or to check the signatures for each other without having to distribute the keys before the intended message is sent.

E. Identity-based encryption applications

The initial purpose of identity-based encryption is to support the establishment of major public infrastructure. More broadly, IBE can improve applications that handle several public keys [13]. The system may either generate these public keys from users or just utilize the integers {1,.....,n} as separate public keys. There are many particular uses discussed below.

F. Public Key Revocation

Public key certificates have an expiry date that has been specified in advance. Alice's e-mail encryption may be forwarded to Bob to use the digital signature: bob@hotmail.com || current year in IBE system key expiry. Bob will only be able to use his private key for the remainder of the current year as a result of this action. Bob requires a fresh PKG private key every year. Therefore, we obtain the yearly expiry of the private key. It should be noted that, in contrast to the current PKI, Alice does not have to acquire a new certificate from Bob each time Bob updates his certificate. Using the email address bob@hotmail.com || current-date, one could make this method more specific by encrypting e-mail for Bob using the current date. This compels Bob every day to get a new private key. This may be achieved in a PKI company, in which the PKG is managed by the company. Once Bob quits the business, the corporate PKG is told to cease providing encryption information for Bob's e-mail address. Alice does not have to interact with any other parties to acquire Bob's daily public key, which is a unique characteristic. This method allows Alice to communicate future messages: Bob can only decode the email on the date indicated by Alice.

G. Delegation of Decryption Keys

Delegation of decryption skills is another aspect for IBE technologies to consider. We'll go over two real-world examples. In both cases, Bob assumes the position of the PKG. Bob uses the setup process to build his own IBE systems settings params, as well as his master key, which he then stores in his computer. In this case, we consider params to be Bob's public key [13]. Bob receives a CA certificate for his public key parameters. Whenever Alice decides to send mail to Bob, she first must get Bob's public key parameters, which she may get from Bob's publicly available key certificate. Because Bob is the only person who has access to his master key, there is no need for key escrow in this configuration [14].

Delegation to a laptop. For example, assuming Alice encrypts mail for Bob using the current time as the IBE encryption key (and Bob's settings as the platform settings for the IBE encrypted file). So long as Bob has the master key, he will be able to obtain the private key that corresponds to this IBE encryption algorithm and use it to read the ciphertext sent to him. Now, assume Bob embarks on a seven-day excursion. Standard practice for

Bob would be to save his encryption key on his computer. If the laptop is stolen, the private key will be exposed. While using the IBE platform, Bob may simply download the seven private keys that corresponded to the 7 days of the excursion and install them on his laptop. It is just the private keys used during those eight days that are vulnerable if the laptop is lost. The master key has not been affected in any way.

Delegation of duties. Consider the following scenario: Alice encrypts a message to Bob that uses the title tag as the IBE encryption key. Bob's master key allows him to decode e-mail. Consider the following scenario: Bob has numerous helpers, each of whom is liable for a distinct duty (for example, one is in charge of procurement, another is in charge of the human resource department, and so on). Bob provides each of his colleagues an individual key that corresponds to the responsibilities of the assistant. Every assistant may then decode communications whose subject lines fall within its duties, but not those meant for other colleagues. It is worth noting that Alice simply receives a single public key from Bob (params), then she utilizes this public key to send an email about any title tag she desires. The email must then be seen by the assistant who is in charge of that particular topic.

H. Identity and Authentication of IAM in an enterprise

Any big or small business continues to rely heavily on passwords, and many firms are unaware of the extent to which implementations are being used. By utilizing b2 cryptography, companies offer a unique tactical edge when authenticating and protecting the identity of cloud users. Following enrollment in the IAM service, a unique ID is generated and connected with a transportable security token based on b2 Encryption that is provided to the user [14]. Clients must have their allocated token on hand as well as the necessary elements of authentication to authenticate. Even though the authentication mechanism is straightforward to use, b2 authentication is resistant to typical threats like brute force, spoofing, identity phishing, SIM switch, man-in-the-middle, and many others. Alternative authentication mechanisms, like smart cards for Windows/Active Directory and single-sign-on, are supported by the IAM service enabling centralized authentication across different platforms (SSO). Such authentication techniques are not recommended, but they can be used as a transitional step to continue functioning user infrastructures and processes running while b2 implementations are being evaluated [15].

I. Encryption of Access Management in enterprises

The IAM service leverages the hierarchical nature of b2 Cryptography to distribute access credentials from higher management to specific users. This hierarchical management structure establishes distinct paths for enforcing access controls that safeguard resources and services. These paths enable managers to decide on roles without IT assistance, at mission speed. Managers are also able to withdraw access and withdraw assigned power. To protect accessibility to more sensitive information or to enforce regulatory compliance, administrators can impose higher authentication requirements on users. Enhanced identification allows people to re-authenticate or provides multiple sources of authentication once permission has been granted to a system or application. The IAM framework enables the use of a combination of up to five different types of authentication [15]. Many businesses currently provide a more secure cloud-based Identity and Access Management service available.

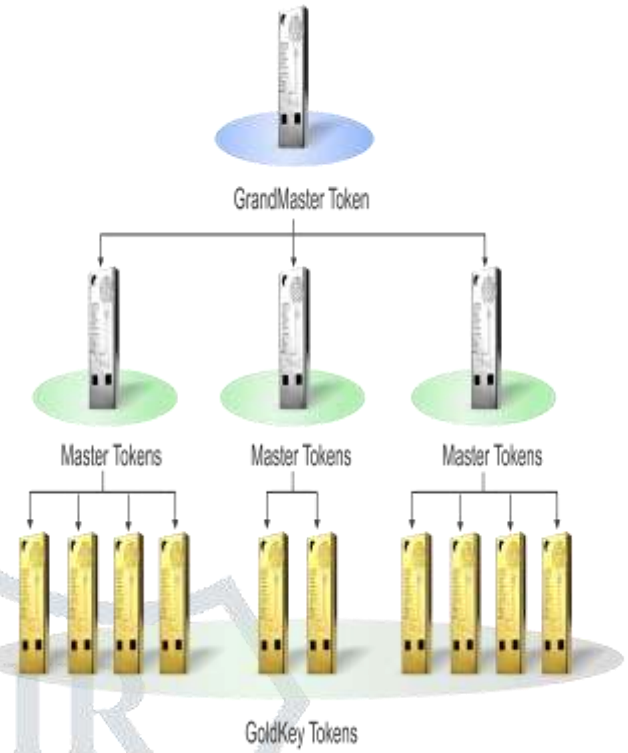

Fig ii: Hierarchical Management with GoldKey® Tokens

IV. FUTURE IN THE U.S

Today, US government agencies generate, analyze and transmit data at an exponentially increasing pace that remains unparalleled. To safeguard all this information – whether it is at rest, in use, or on the go – the government should not only utilize the most dependable encryption technology of the day but must also be prepared for its adoption tomorrow. As the dangers of insiders and opponents increase and develop, it is important to preserve the nation's information security by offering new methods to encryption – such as after-quantum encryption, quantum key distribution, and homomorphic encryption [16]. Emerging encryption technologies will be essential in ensuring the government's digital ecosystems safe growth and development. While organizational requirements differ, sophisticated encryption is essential to every modernized digital infrastructure. In the next years, postquantum encryption will be necessary for workplaces with data that have to be secured after initial encryption for a long time [17].

V. ECONOMIC GAINS

The National Institute of Standards and Technology (NIST) of the United States Department of Commerce has published research that predicts a $250 billion economic benefit from the creation of its Advanced Encryption Standard (AES) over the last 20 years. AES is an encrypted technique used for electronic information encryption and decryption [17,18]. The federal government authorized its usage in November 2001, and private business has subsequently extensively embraced it. For instance, without robust cryptographies, the $40 million and more trillions in online banking industries were "seriously disrupted" and online purchases totaling $3.3 trillion in 2013 relied on confidence and security cryptography [18].

AES is now used to secure anything from sensitive information and financial operations to online digital technologies and social networking applications, among other things. The current research shows that NIST investment in AES has been reimbursed many times with economic gains that surpass its expenditures. The AES program has a 29-to-1 benefit-to-cost ratio, according to the research [18,19]. The

projected benefit/cost ratio is 1,976-to-1 for the whole economy. The evaluation covers the years 1996-2016. This excellent return on investment illustrates the economic benefit for the private industry and wider American economy of government design and technology [16]. Additionally, it shows how successfully bringing the private and governmental sectors together to solve a problem may have a beneficial influence on US trade. A fierce and highly technical fight has raged between the US government with America's industry figures for the last five years over cryptographic plan: the game rules for methods used to disguise and decode data [19]. This decryption process is critical for preserving the security of information (whether corporate information, cash transactions, individual medical data, or classified information) flowing across the nation's expanding network of data and telecommunications connections. The difficult and sometimes esoteric discussion has led to an inconclusive and unsatisfactory drawing that does nothing to address any competing goals — civil rights, economic success, regulation, and national security — at a negotiating table. In military institutions, which originally stimulated the computer industry, similarly, significant changes are taking place.

VI. CONCLUSION

This paper explored how identity-based encryption is a vital tool in identity access management and enterprise privacy. The study indicates that identity-based encryption is an essential tool to safeguard the business from unwanted access, which may lead to sensitive information and money loss. Adi Shamir was called upon to develop the IBE idea in 1984 because of the necessity for a certified and secure connection. The first to develop a fully functioning IBE methodology based on the Weil pairing followed the concept of Dan Boneh and Matt Franklin. The fundamental concept underlying their method is the utilization of the information sources about the recipient's identification, such as an E-mail address or telephone number, to quickly create the public key without having to contact the key server or recipient. Organizations in this area specialize in the storage and management of software, infrastructure, cloud solutions, and permission levels. These technologies restrict access from outside parties and prevent individuals from reaching files and programs which are beyond their privileges. The fundamental reason for identity-based cryptography is to assist deploy an infrastructure of public importance. IBE may simplify systems that handle a wide range of public keys more broadly. Instead of maintaining a large public key database, the system may either extract these public keys from users or just utilize the integer.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", Proc. of Advances in Cryptology - Crypto '84, pp. 47-53, 1985.

[2] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing", Proc of Advances in Cryptology - Crypto 2001, pp. 213-229, 2001.

[3] K. Chalkias, D. Hristu-Varsakelis and G. Stephanides, "Improved Anonymous Timed-Release Encryption", ESORICS 07, pp. 311-326, 2007.

[4] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in Public Key Cryptography—PKC 2005, S. Vaudenay, Ed., pp. 362–379, Springer, Berlin, Germany, 2005.

[5] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in Proceedings of the 30th Annual Conference on Advances in Cryptology. CRYPTO'10, pp. 98–115, Springer-Verlag, Santa Barbara, CA, USA, August,2010,http://dl.acm.org/citation.cfm?id=1881412.1881420.

[6] D. Boneh, X. Boyen, and E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Advances in Cryptology—EUROCRYPT 2005, R. Cramer, Ed., pp. 440–456, Springer, Berlin, Germany, 2005.

[7] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proceedings of the fourtieth annual ACM symposium on Theory of computing—STOC 08, pp. 197–206, ACM, Victoria, Canada, May 2008.

[8] B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology—EUROCRYPT 2005, R. Cramer, Ed., pp. 114–127, Springer, Berlin, Germany, 2005.

[9] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Advances in Cryptology—ASIACRYPT 2005, B. Roy, Ed., pp. 515–532, Springer, Berlin, Germany, 2005.

[10] F. Hess, "Efficient identity based signature schemes based on pairings," in Selected Areas in Cryptography, K. Nyberg and H. Heys, Eds., pp. 310–324, Springer, Berlin, Germany, 2003.

[11] K. G. Paterson and J. C. N. Schuldt, "Efficient identity-based signatures secure in the standard model," in Information Security and Privacy, L. M. Batten and R. Safavi-Naini, Eds., pp. 207–222, Springer, Berlin, Germany, 2006.

[12] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in Post-quantum Cryptography, N. Sendrier, Ed., pp. 182–200, Springer, Berlin, Germany, 2010.

[13] J. Xie, Y.-P. Hu, J.-T. Gao, and W. Gao, "Efficient identity-based signature over ntru lattice," Frontiers of Information Technology & Electronic Engineering, vol. 17, no. 2, pp. 135–142, 2016.

[14] X. Boyen, "Multipurpose identity-based signcryption," in Advances in Cryptology—CRYPTO 2003, D. Boneh, Ed., pp. 383–399, Springer, Berlin, Germany, 2003.

[15] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for NTRUEncrypt," Cryptology ePrint Archive, Report 2015/708, 2015, https://eprint.iacr.org/2015/708.

[16] L. Ducas, V. Lyubashevsky, and T. Prest, "Efficient identity-based encryption over NTRU lattices," in Advances in Cryptology—ASIACRYPT 2014, P. Sarkar and T. Iwata, Eds., pp. 22–41, Springer, Berlin, Germany, 2014.

[17] M. Albrecht, S. Bai, and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions," in Advances in Cryptology—CRYPTO 2016, M. Robshaw and J. Katz, Eds., pp. 153–178, Springer, Berlin, Germany, 2016.

[18] J. H. Cheon, J. Jeong, and C. Lee, "An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero," LMS Journal of Computation and Mathematics, vol. 19, no. A, pp. 255–266, 2016.

[19] D. Stehlé and R. Steinfeld, "Making ntruencrypt and ntrusign as secure as standard worst-case problems over ideal lattices," Cryptology ePrint Archive, Report 2013/004, 2013, https://eprint.iacr.org/2013/004.